

Fig. 1A
(Prior Art)

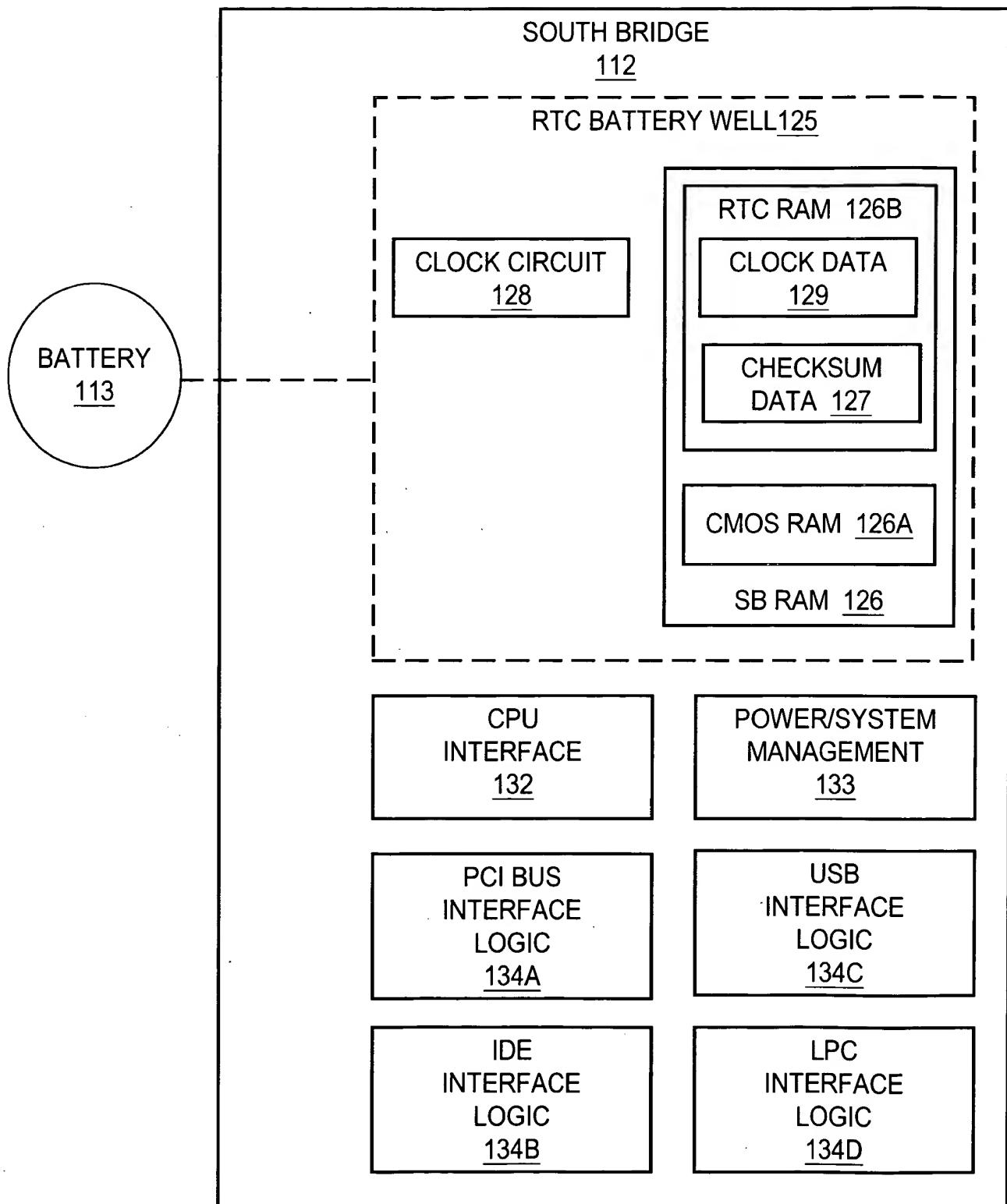


Fig. 1B
(Prior Art)

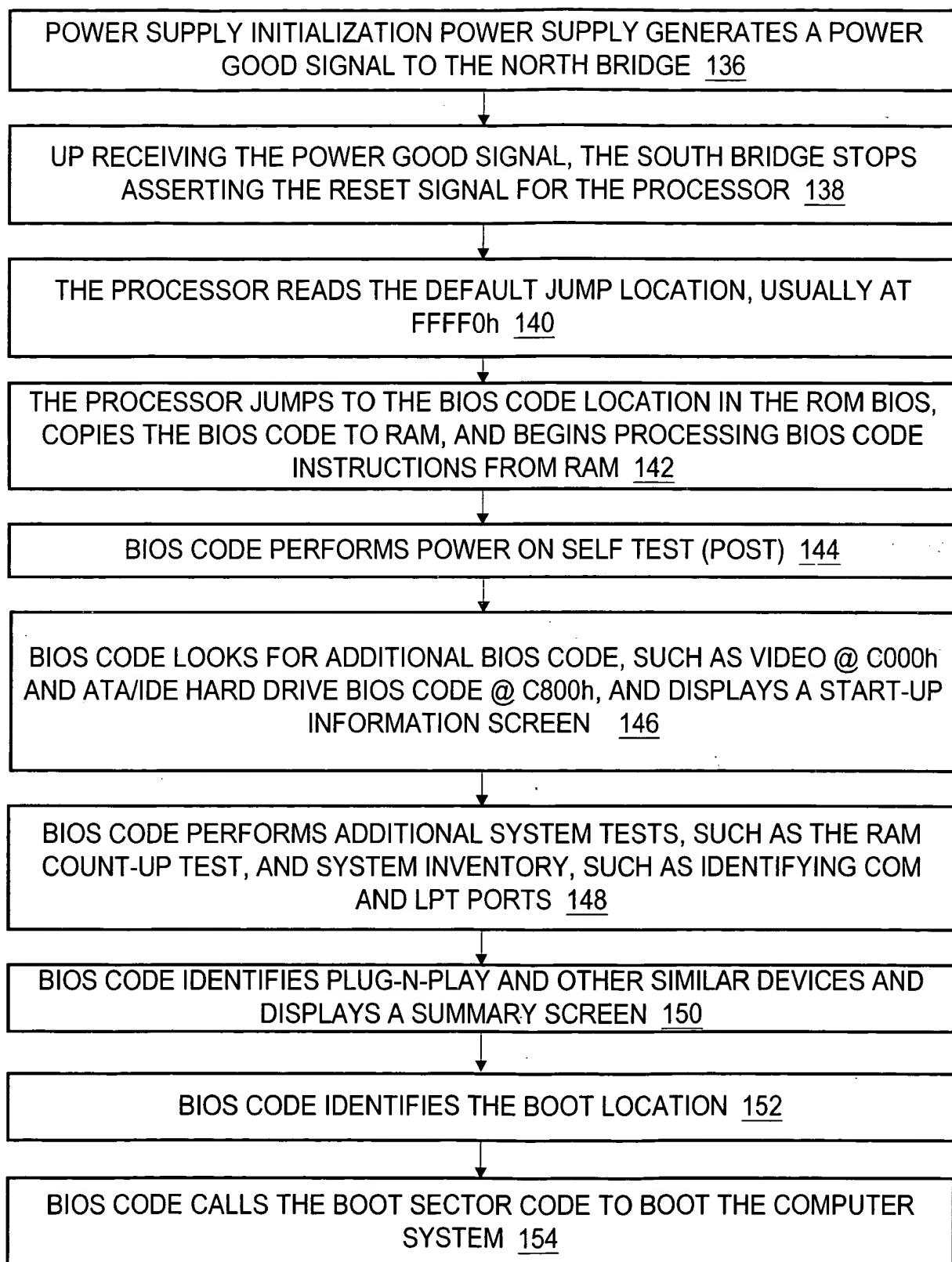


Fig. 2A
(Prior Art)

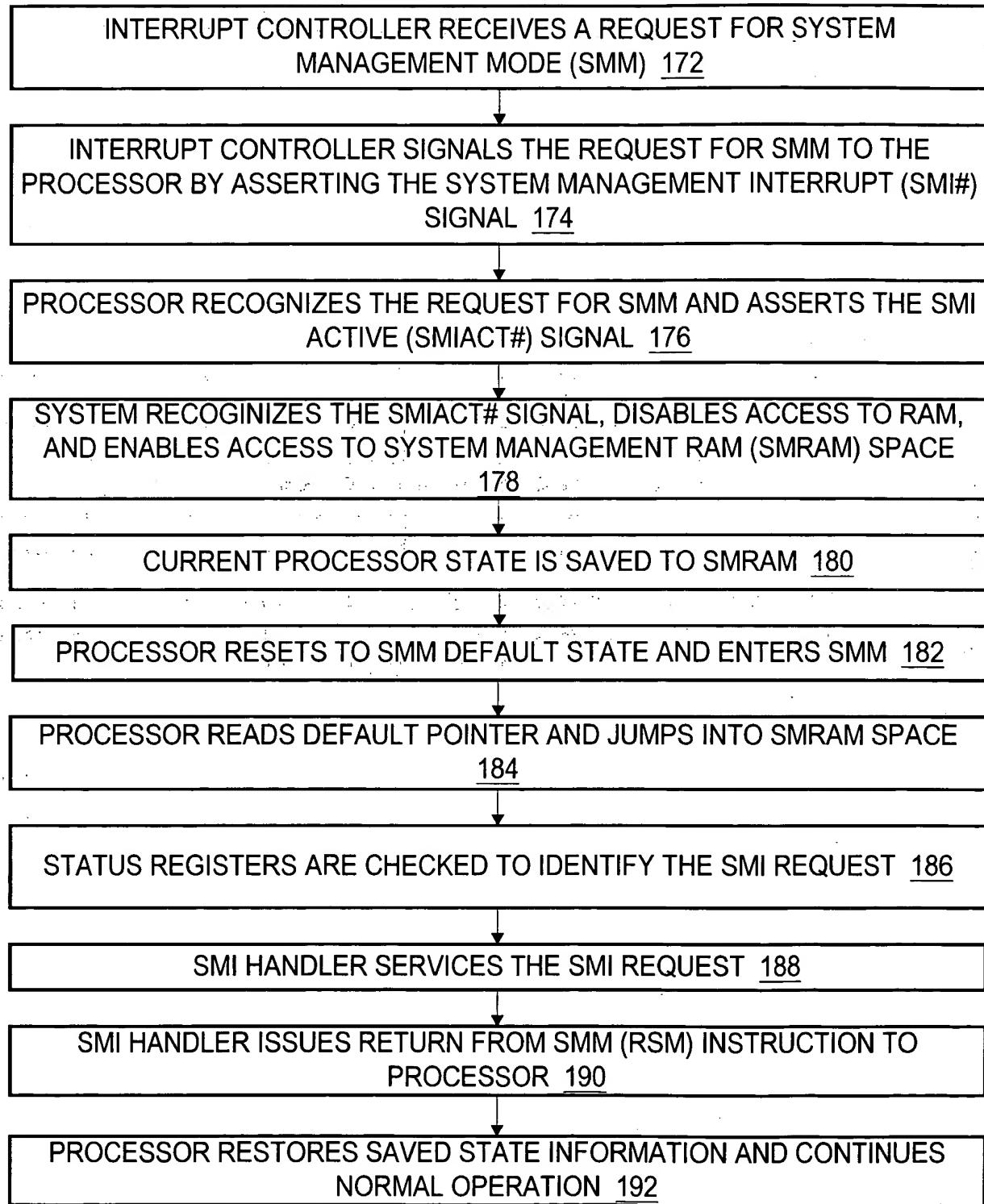


Fig. 2B
(Prior Art)

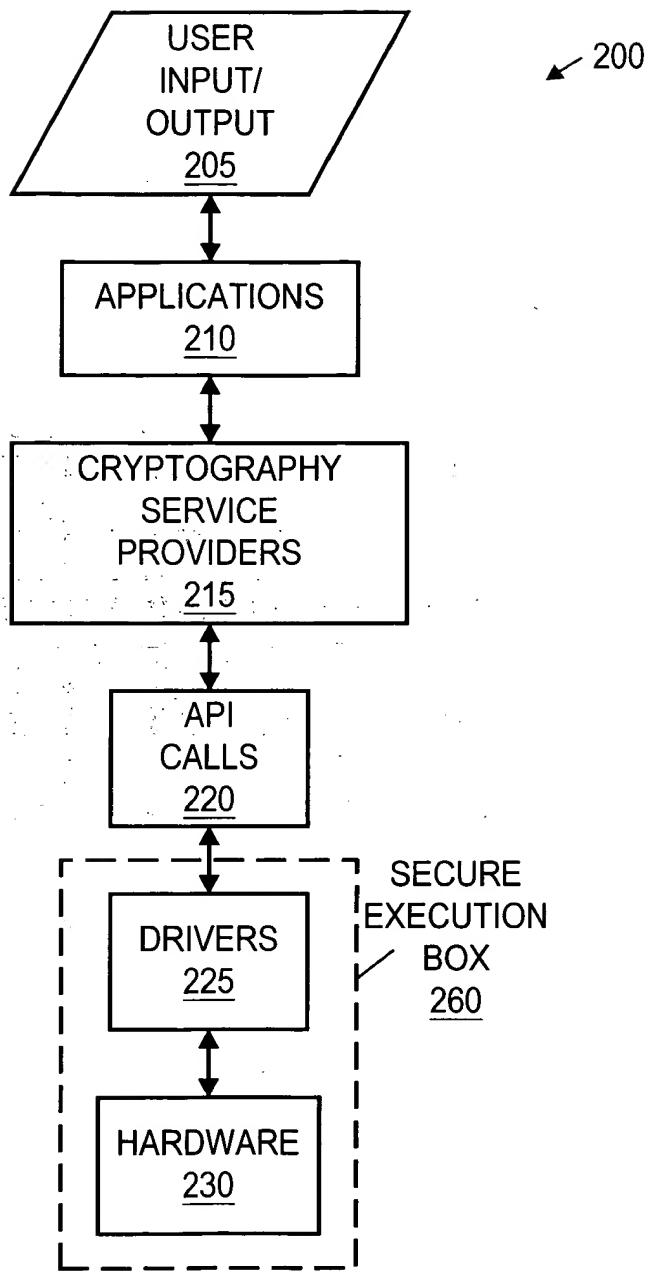
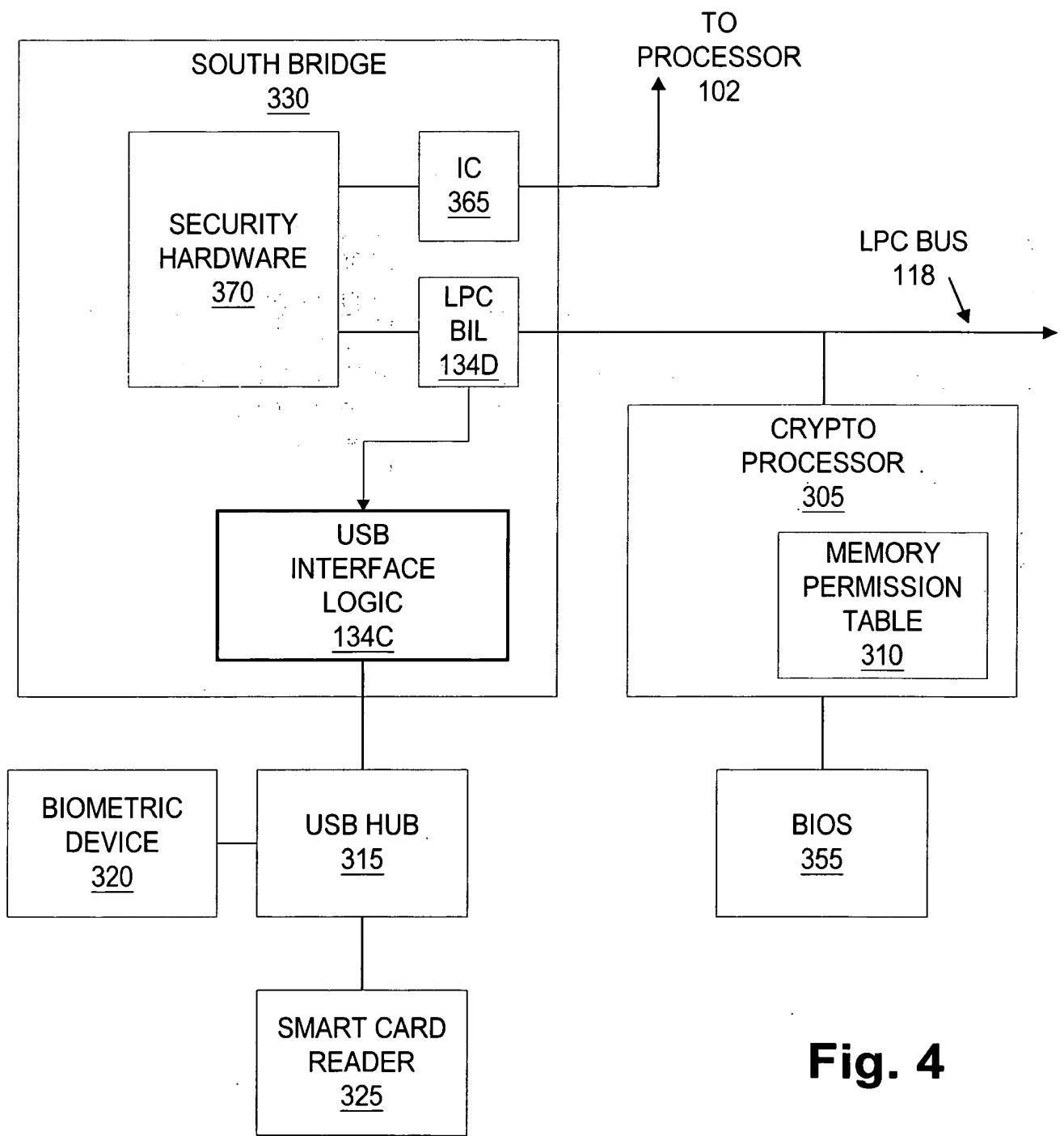
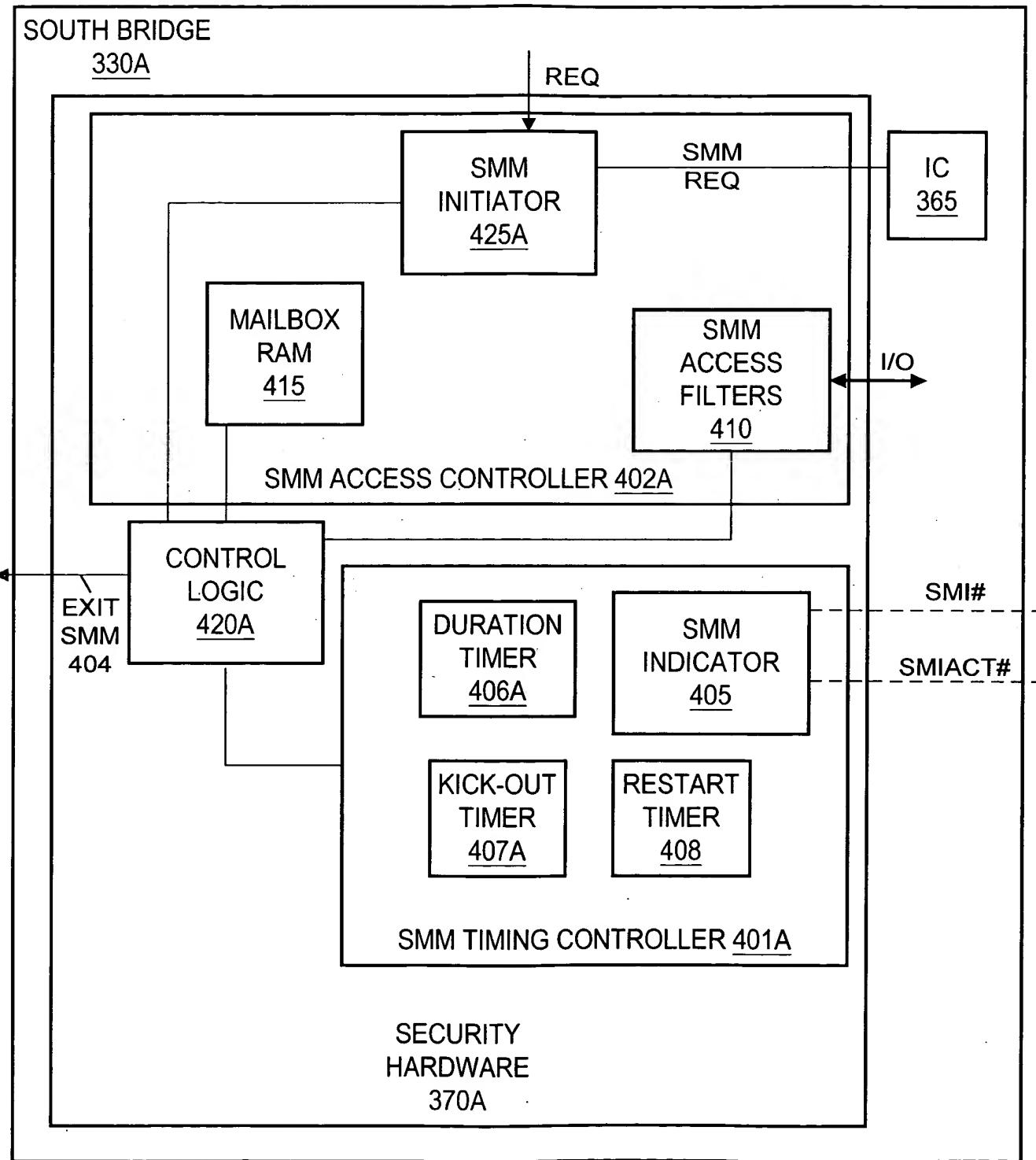


Fig. 3

**Fig. 4**

**Fig. 5A**

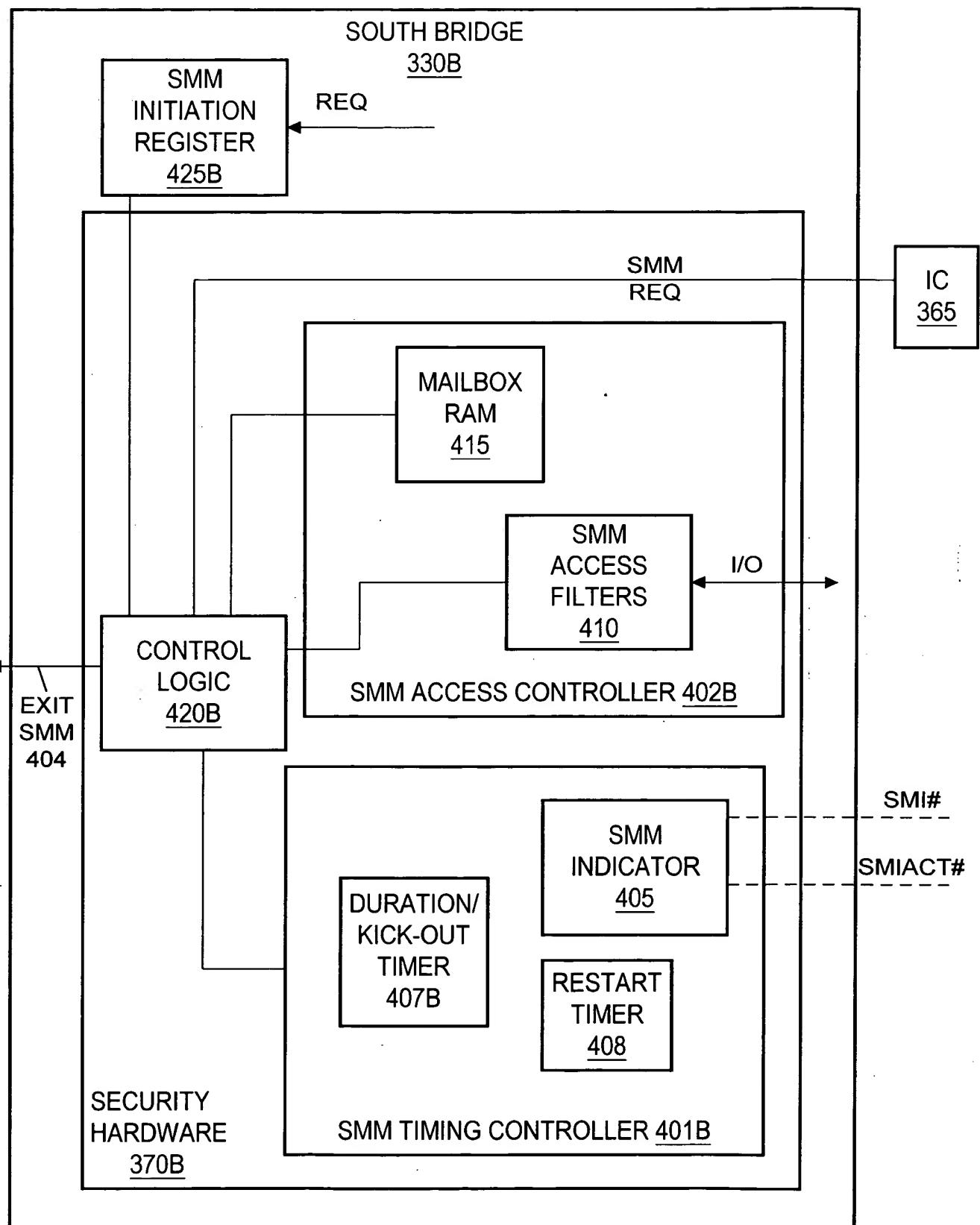


Fig. 5B

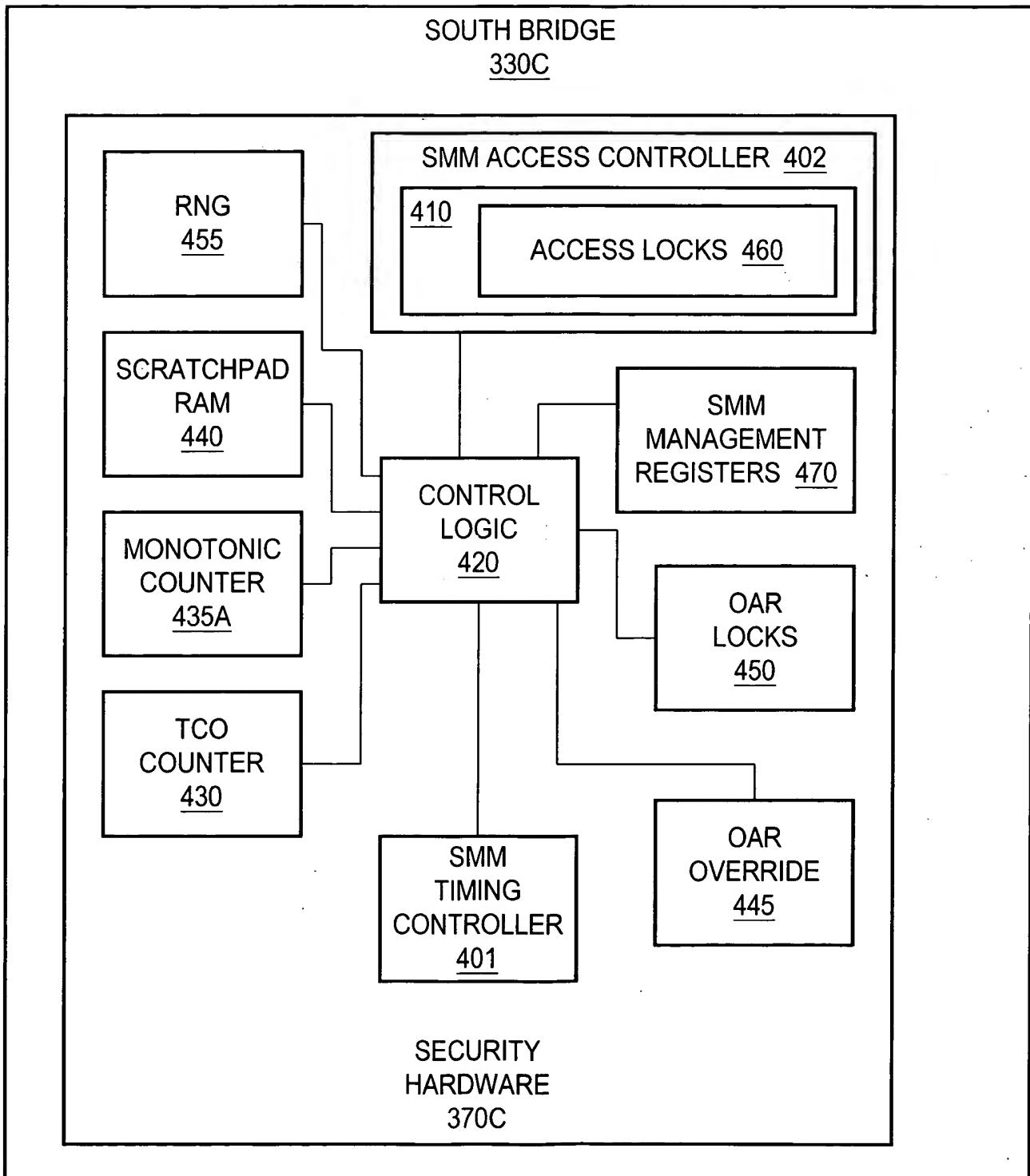


Fig. 6

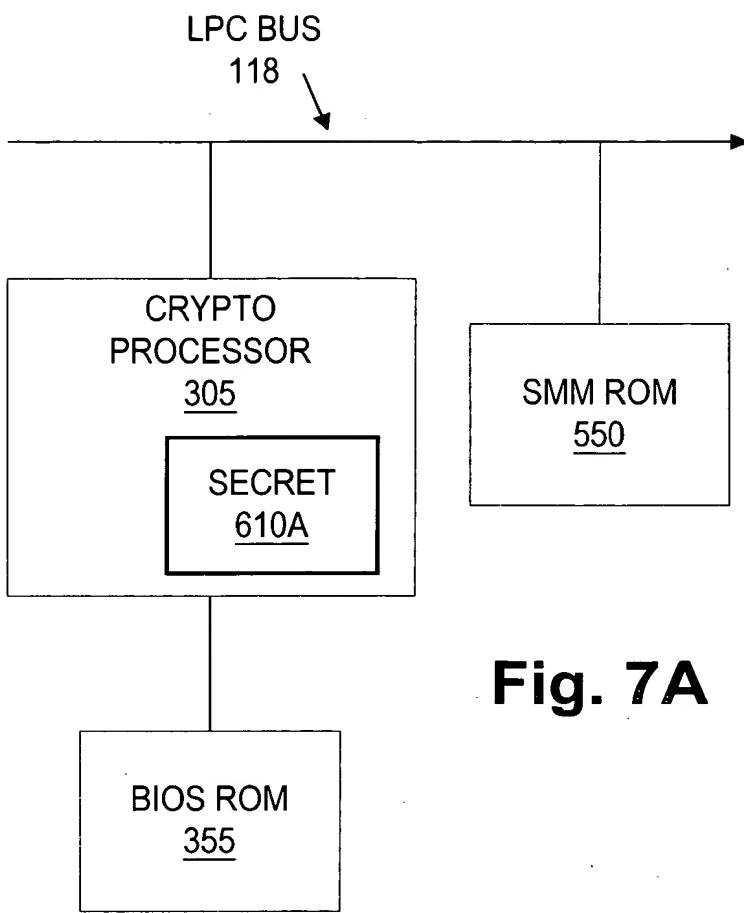


Fig. 7A

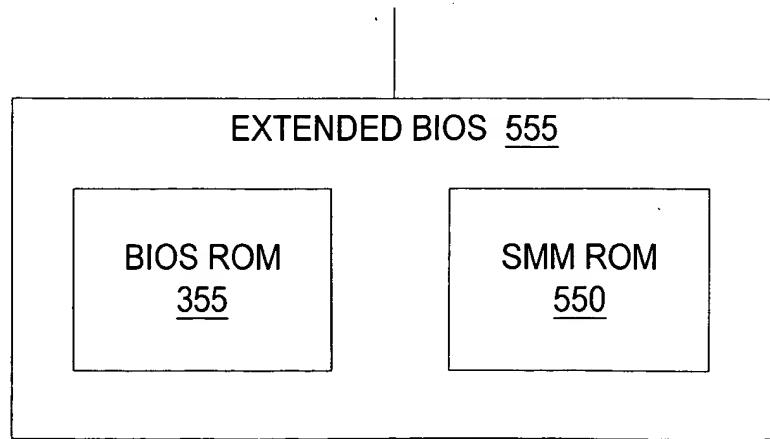


Fig. 7B

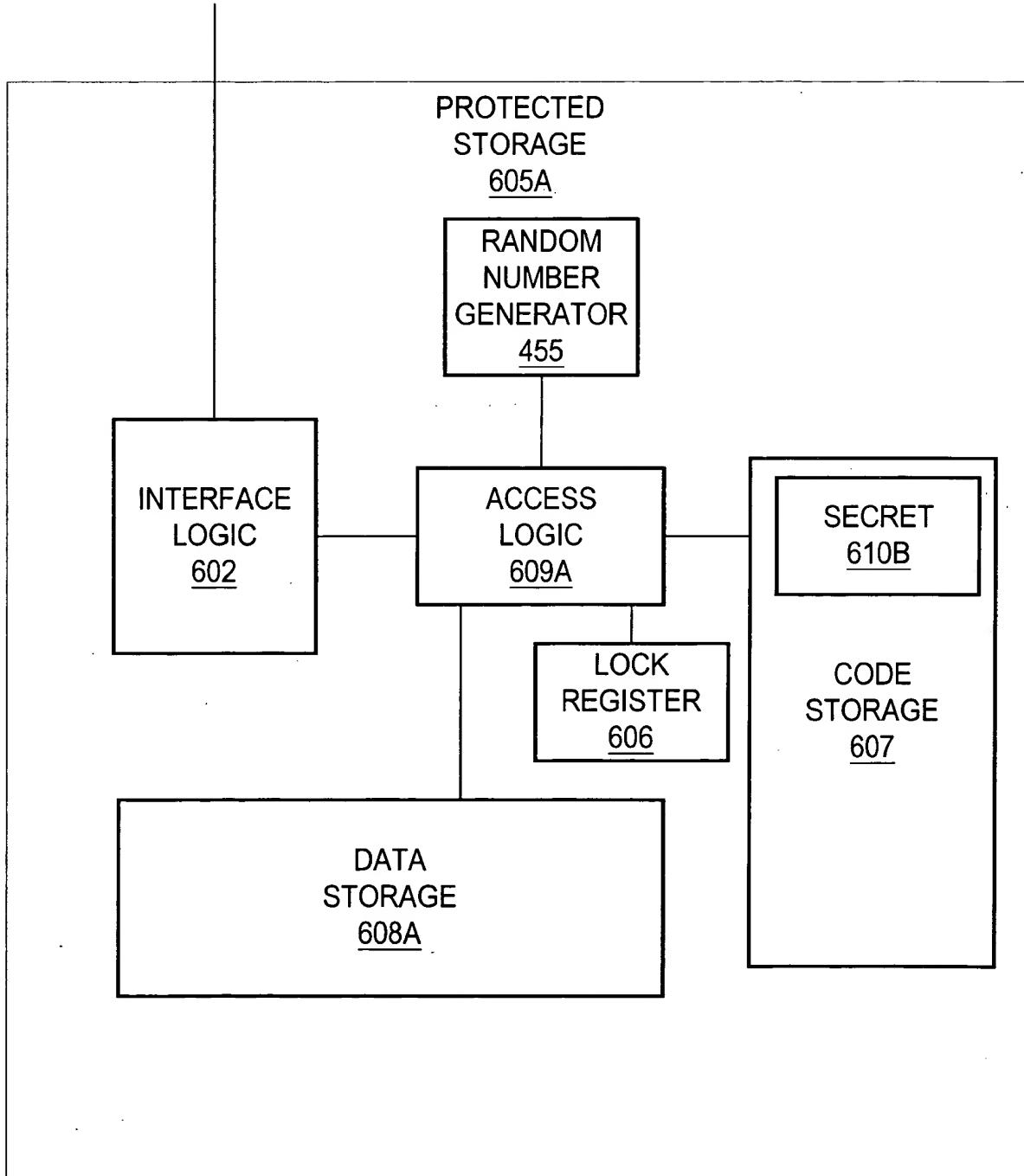


Fig. 7C

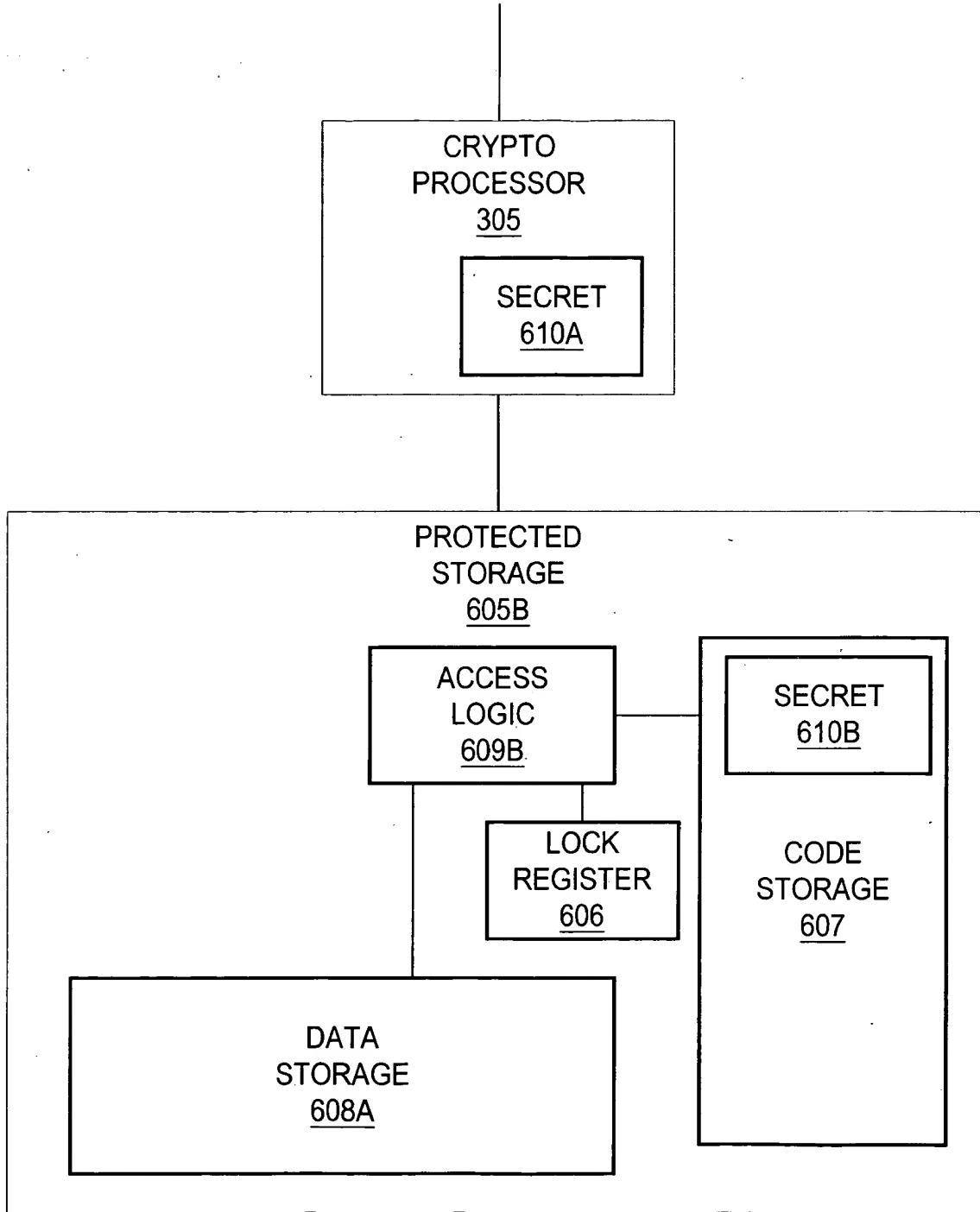


Fig. 7D

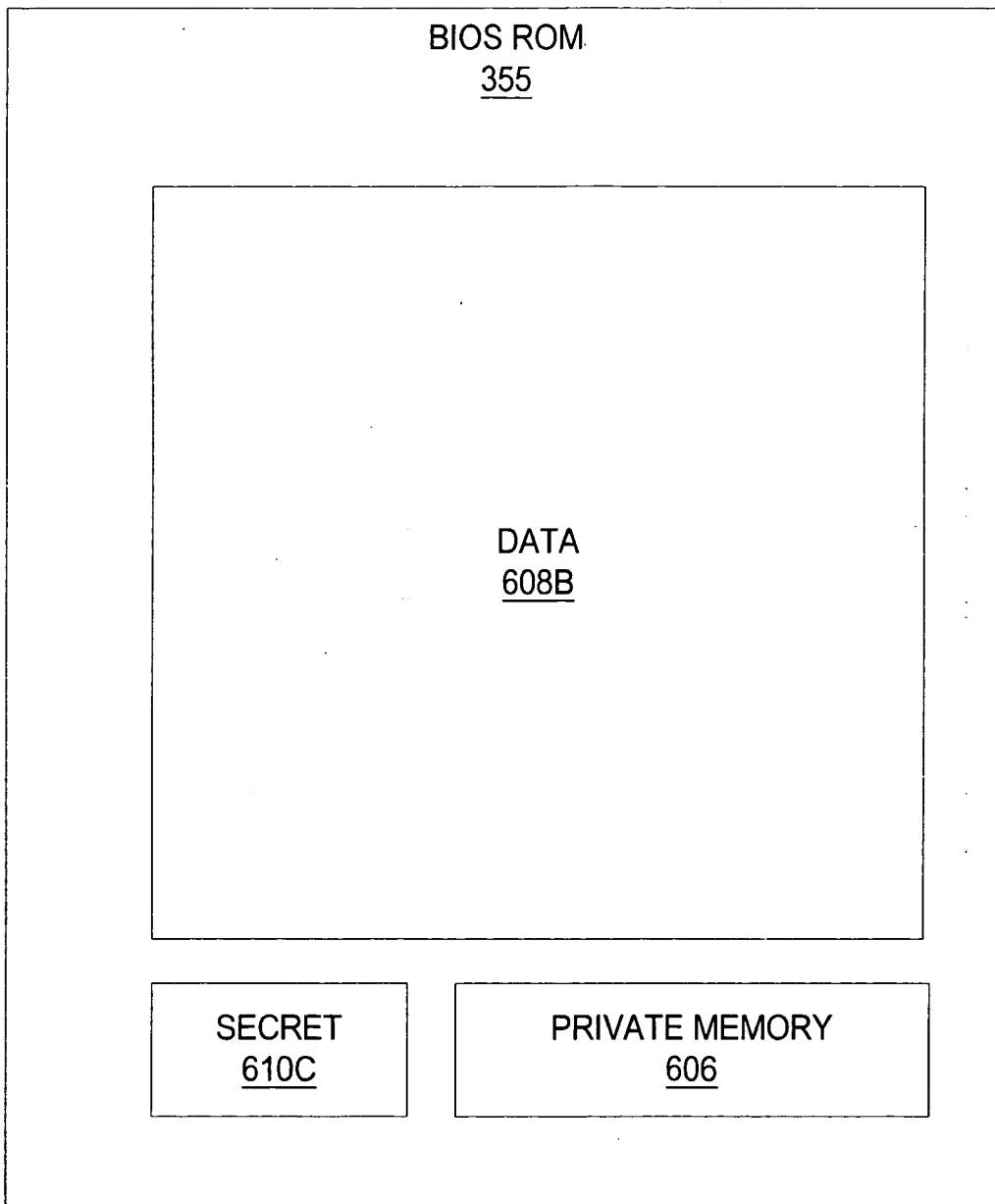


Fig. 8A

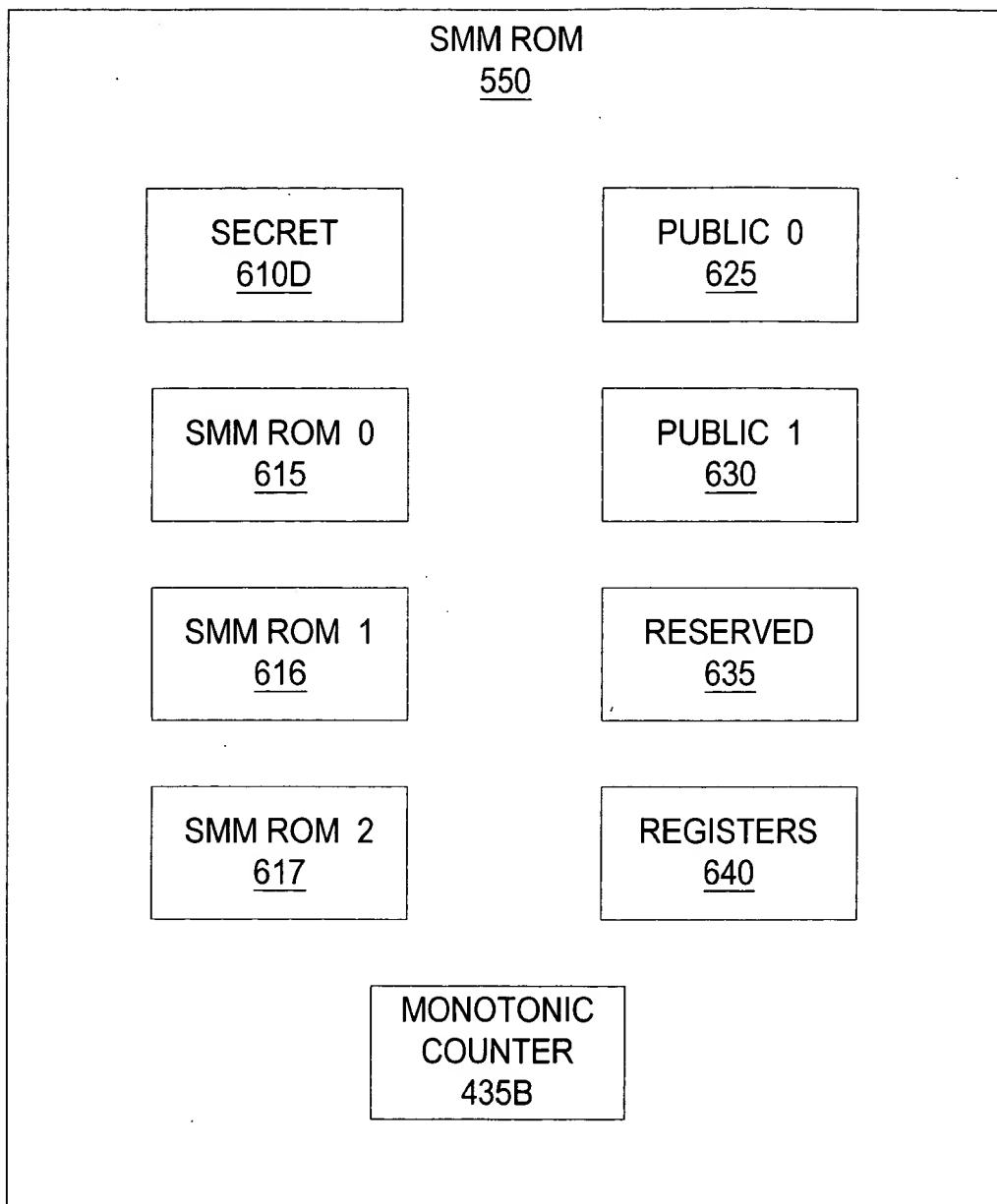


Fig. 8B

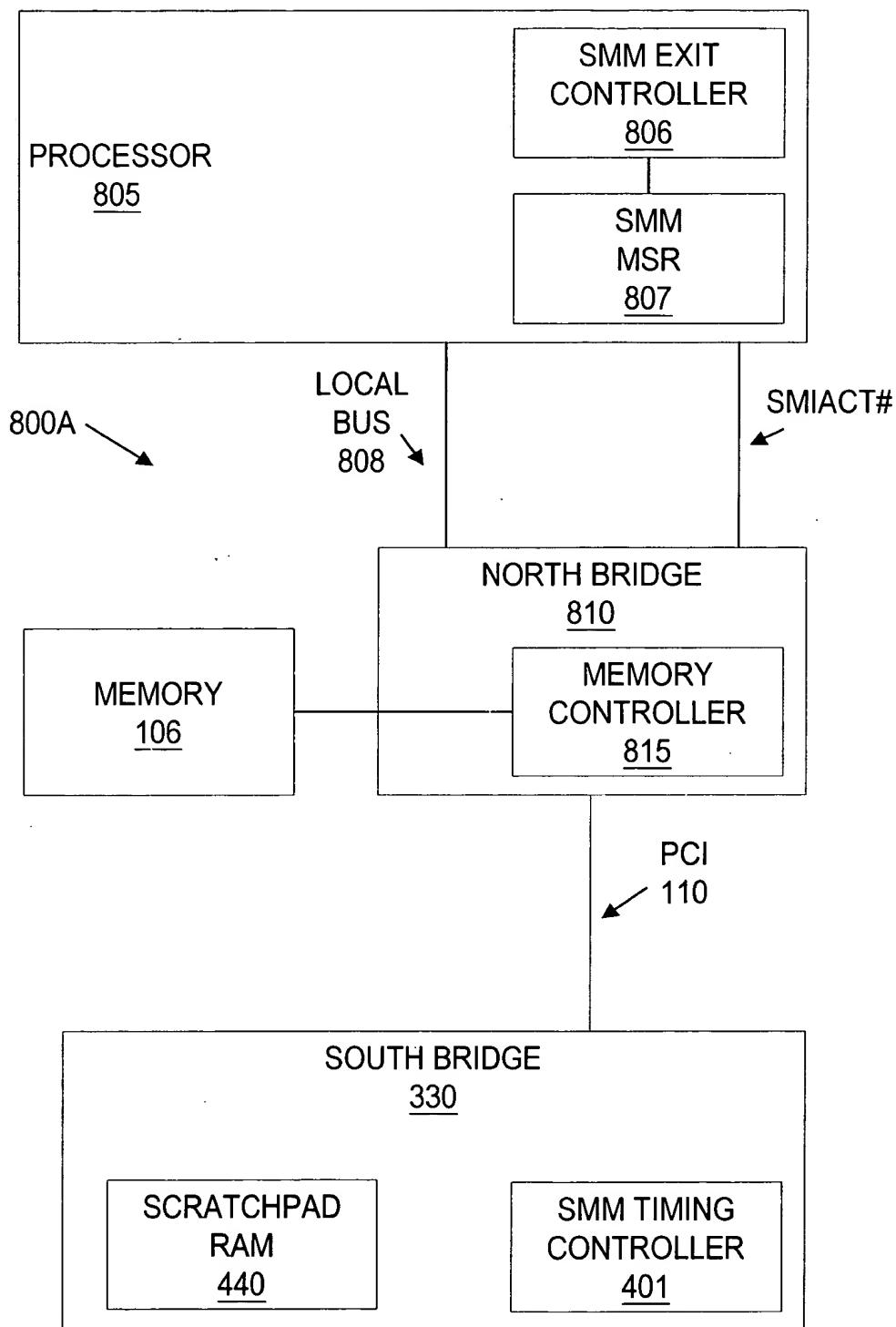


Fig. 9A

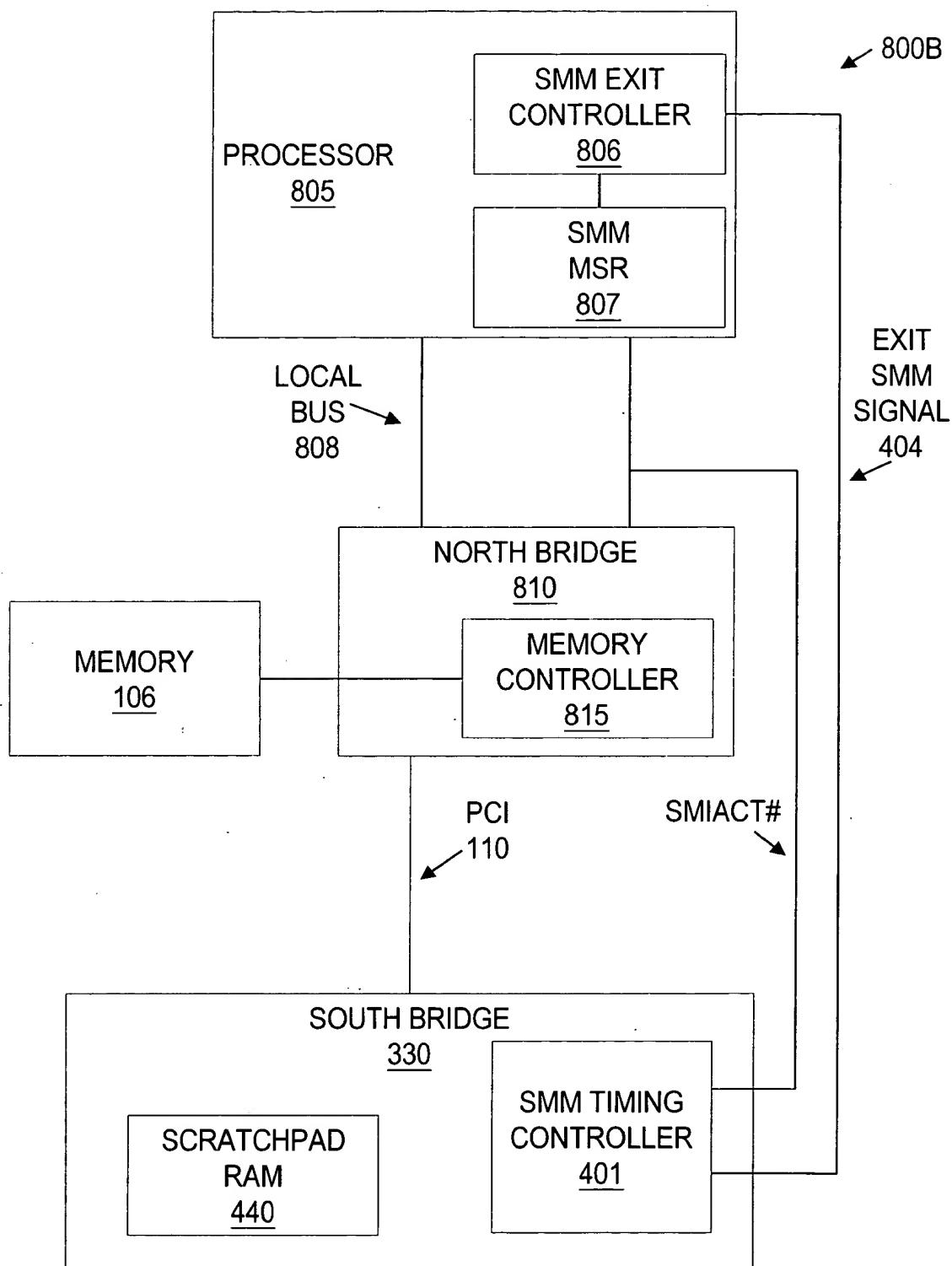


Fig. 9B

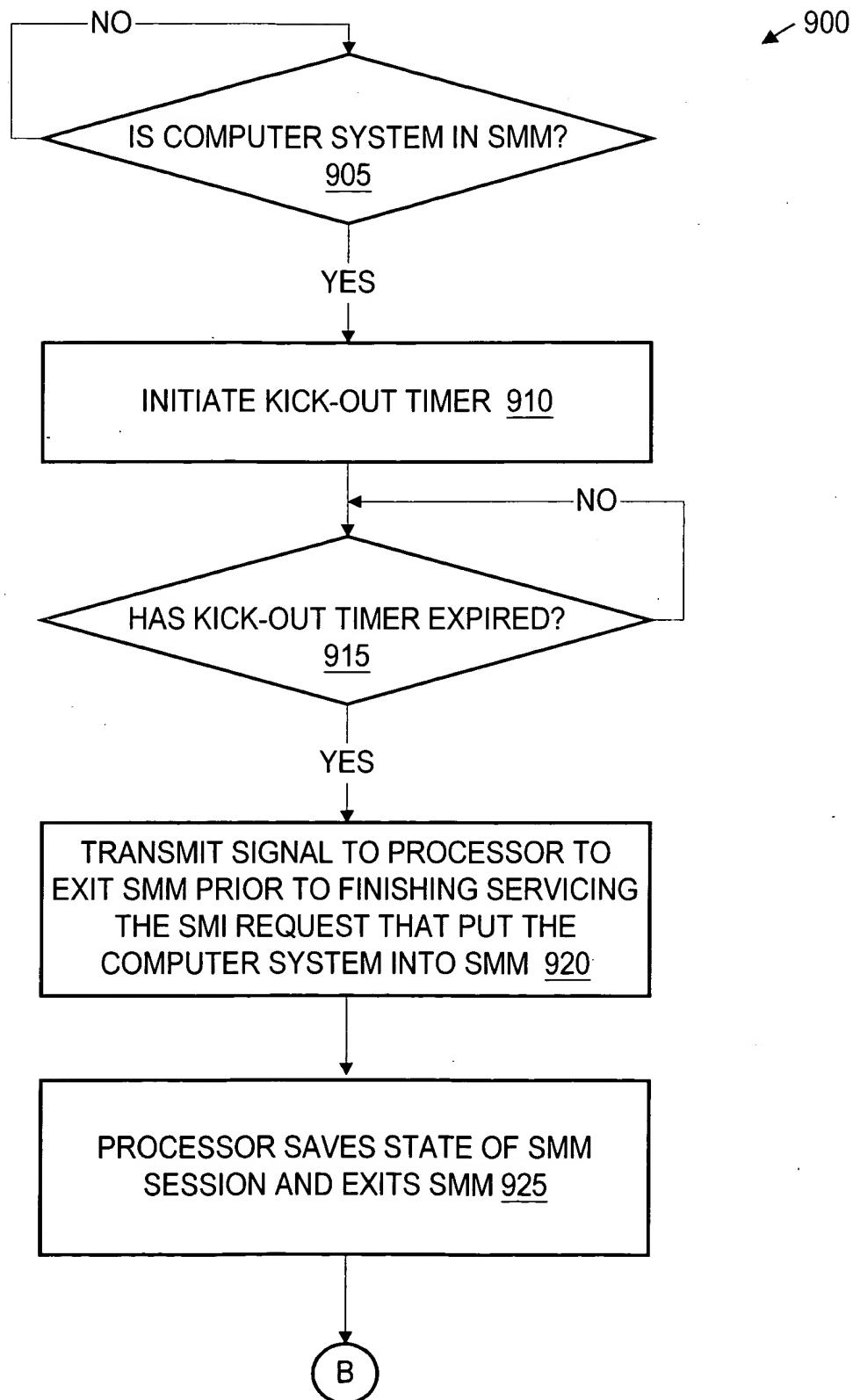


Fig. 10A

18 / 73

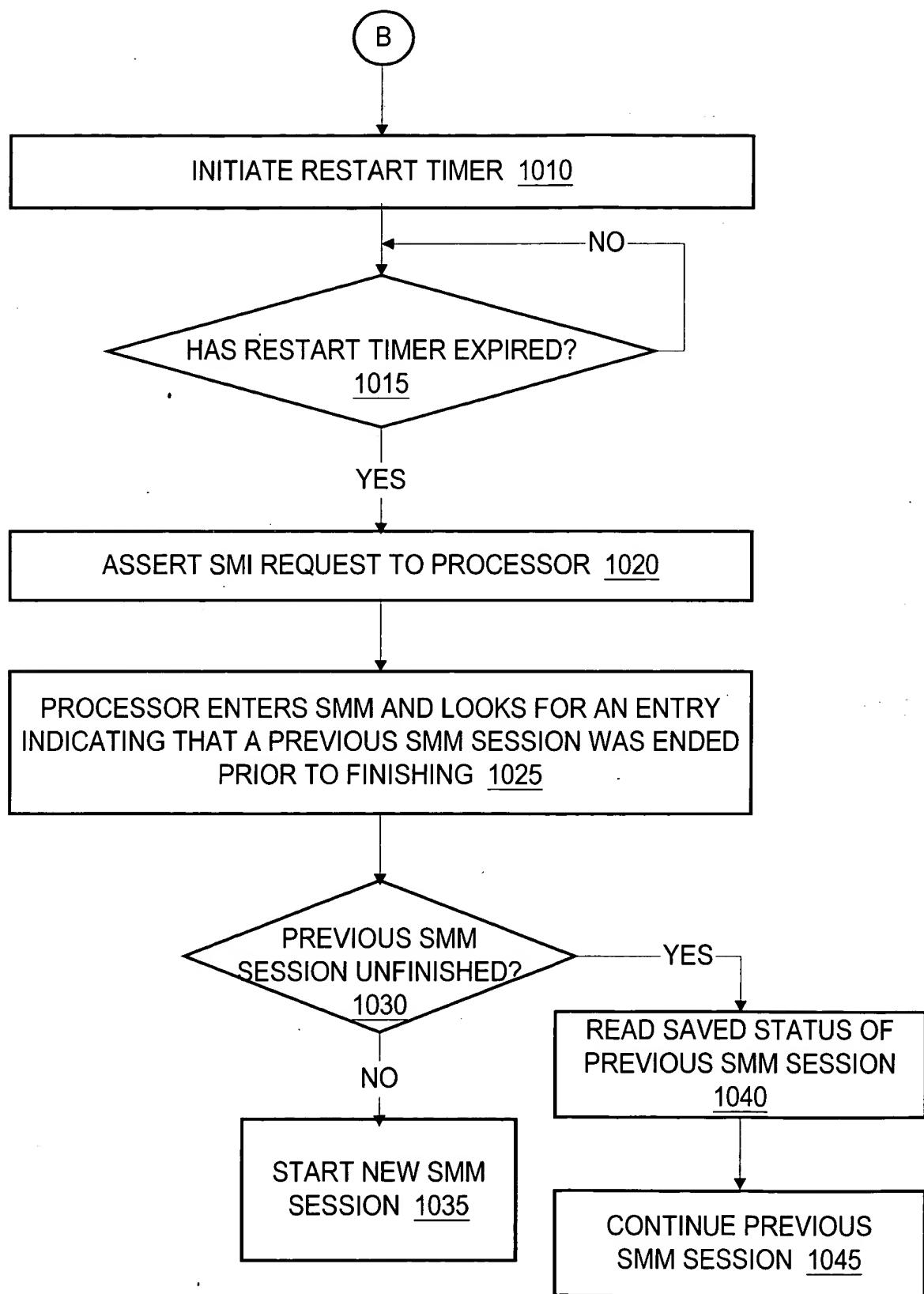


Fig. 10B

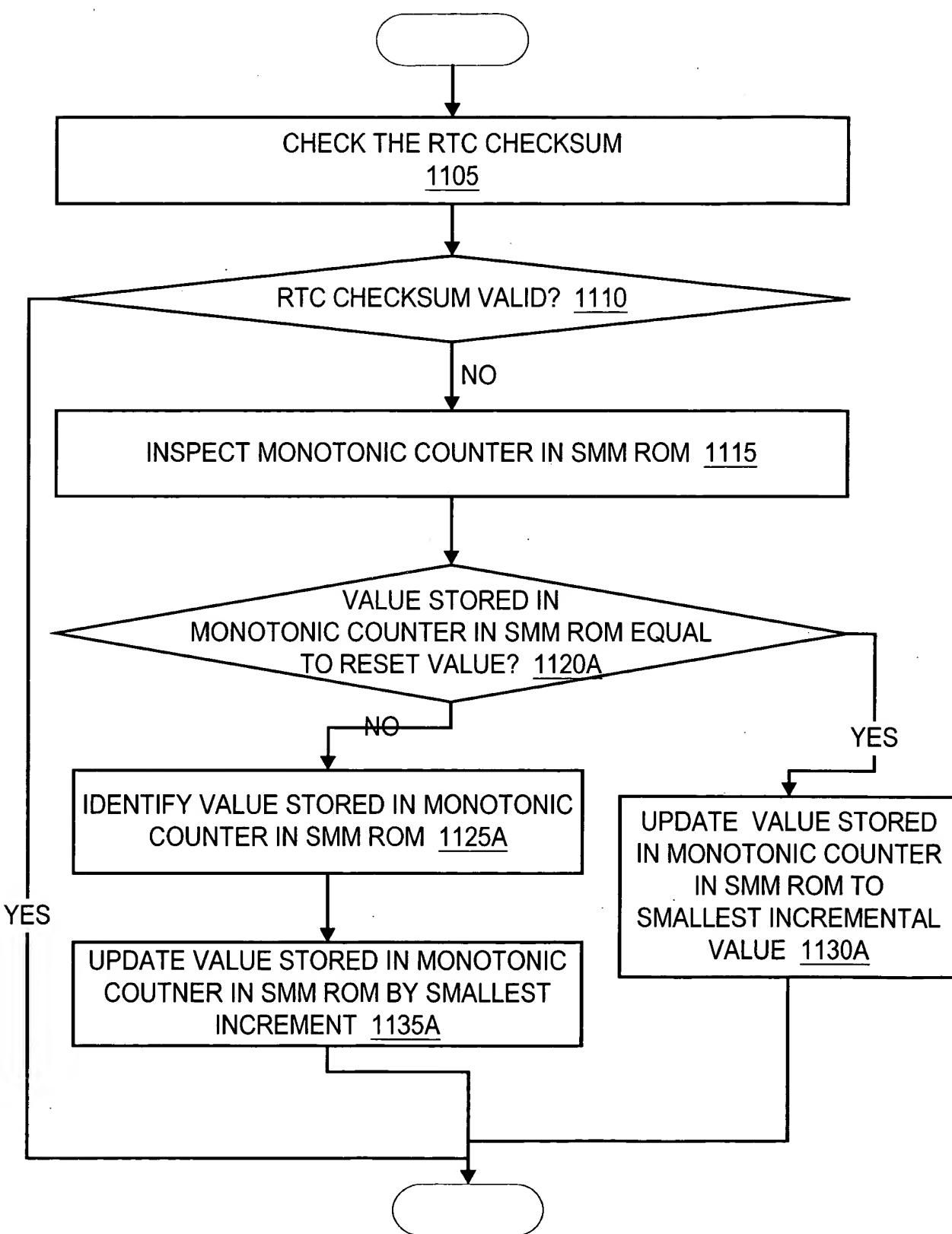


Fig. 11A

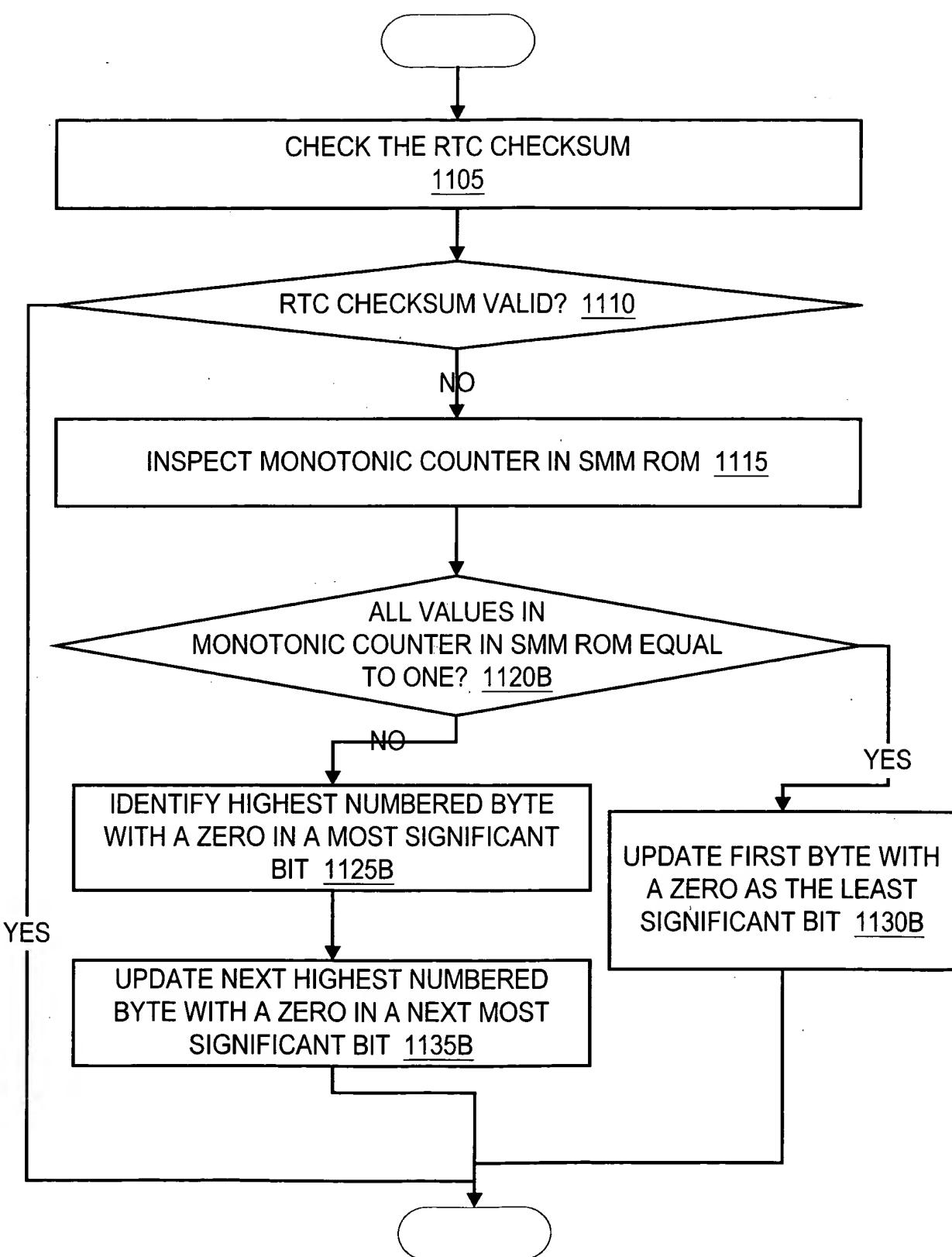


Fig. 11B

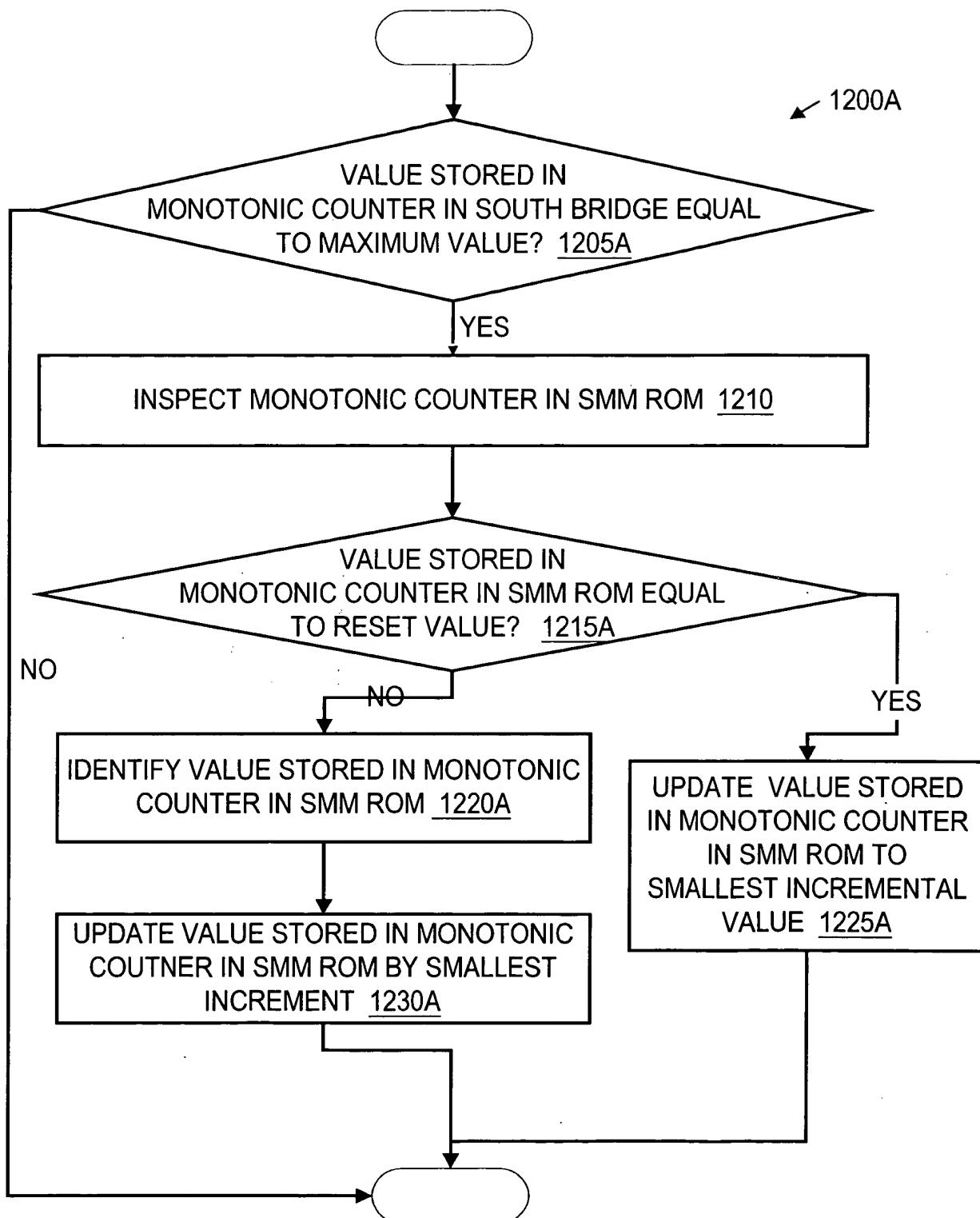


Fig. 12A

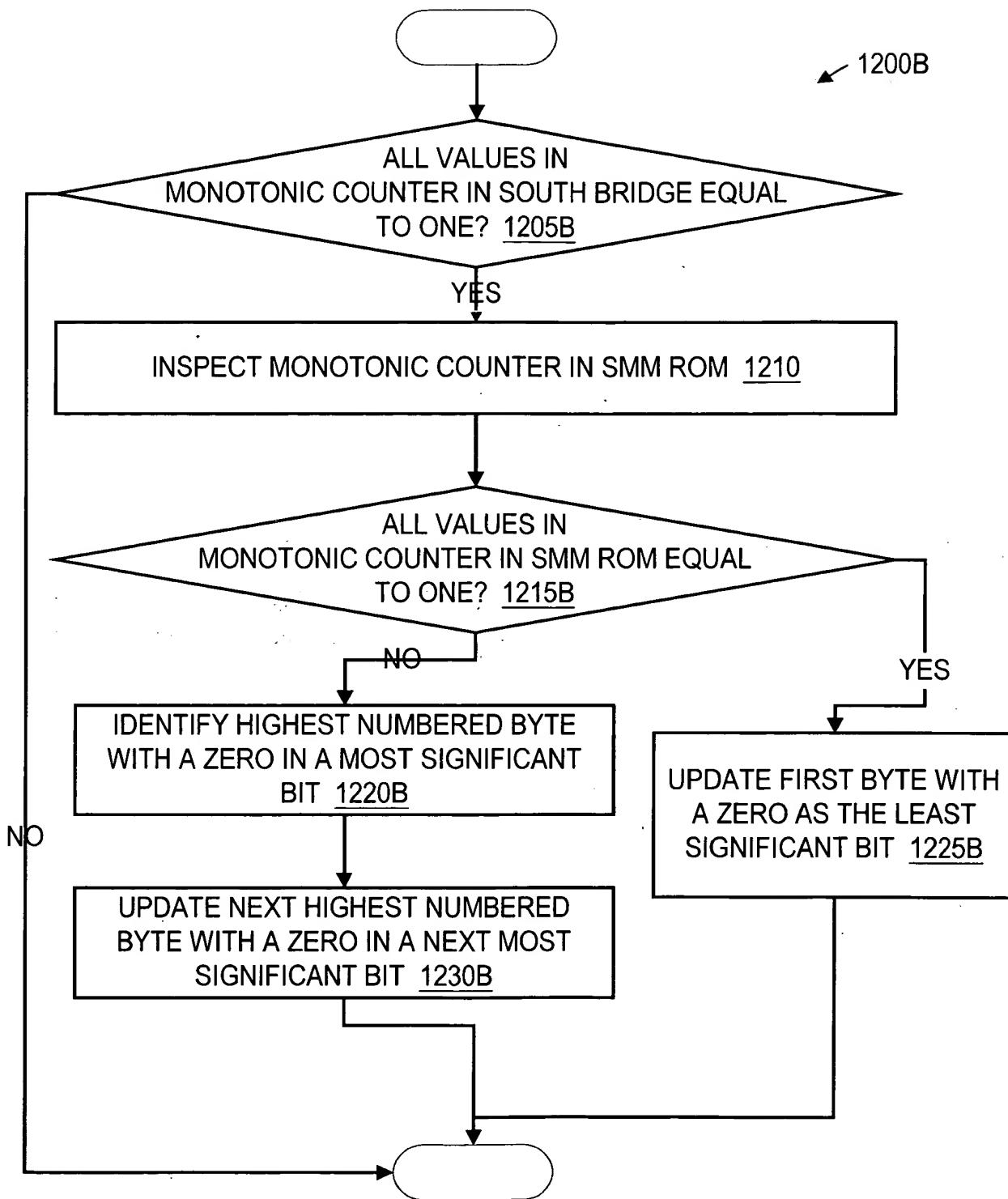


Fig. 12B

23 / 73

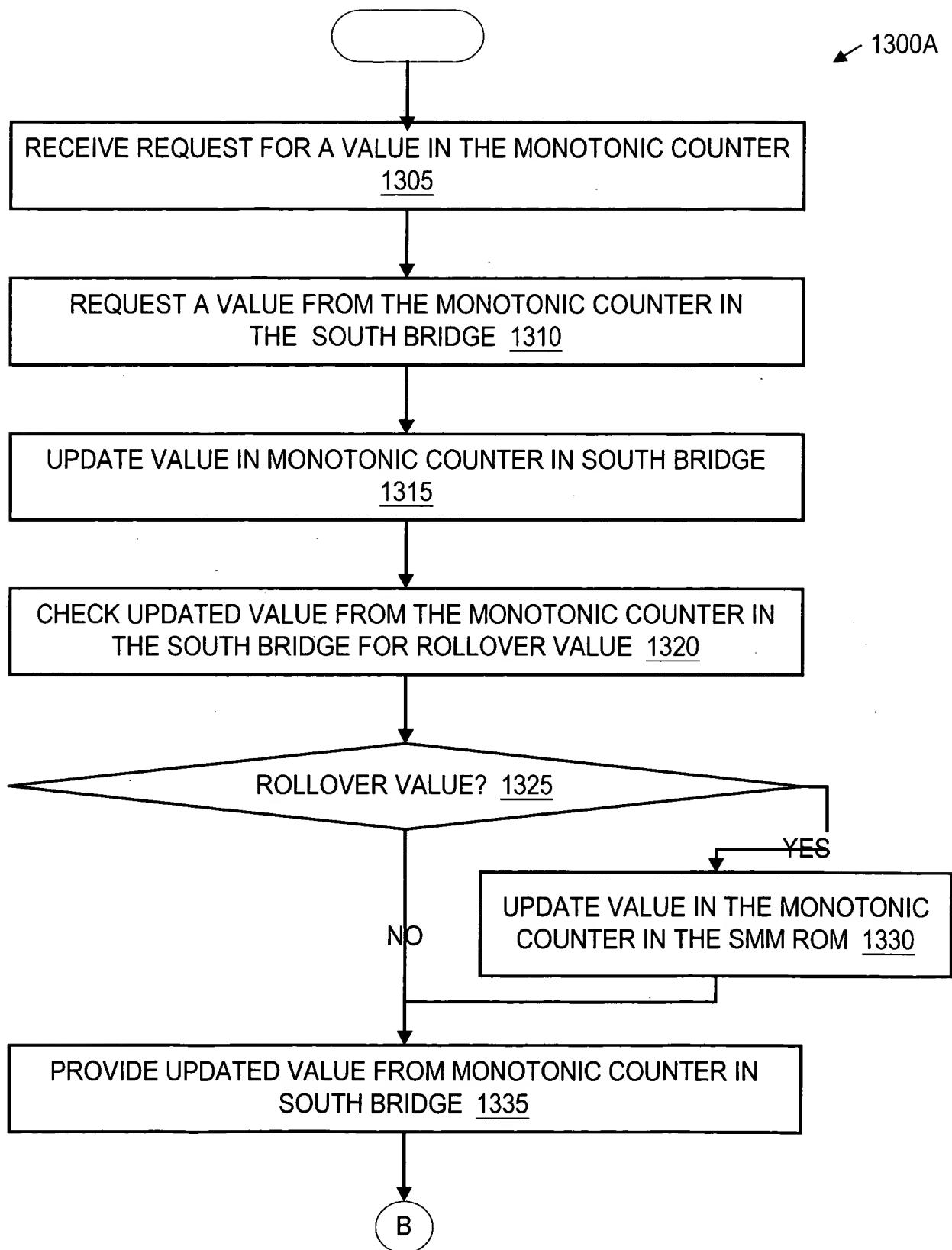


Fig. 13A

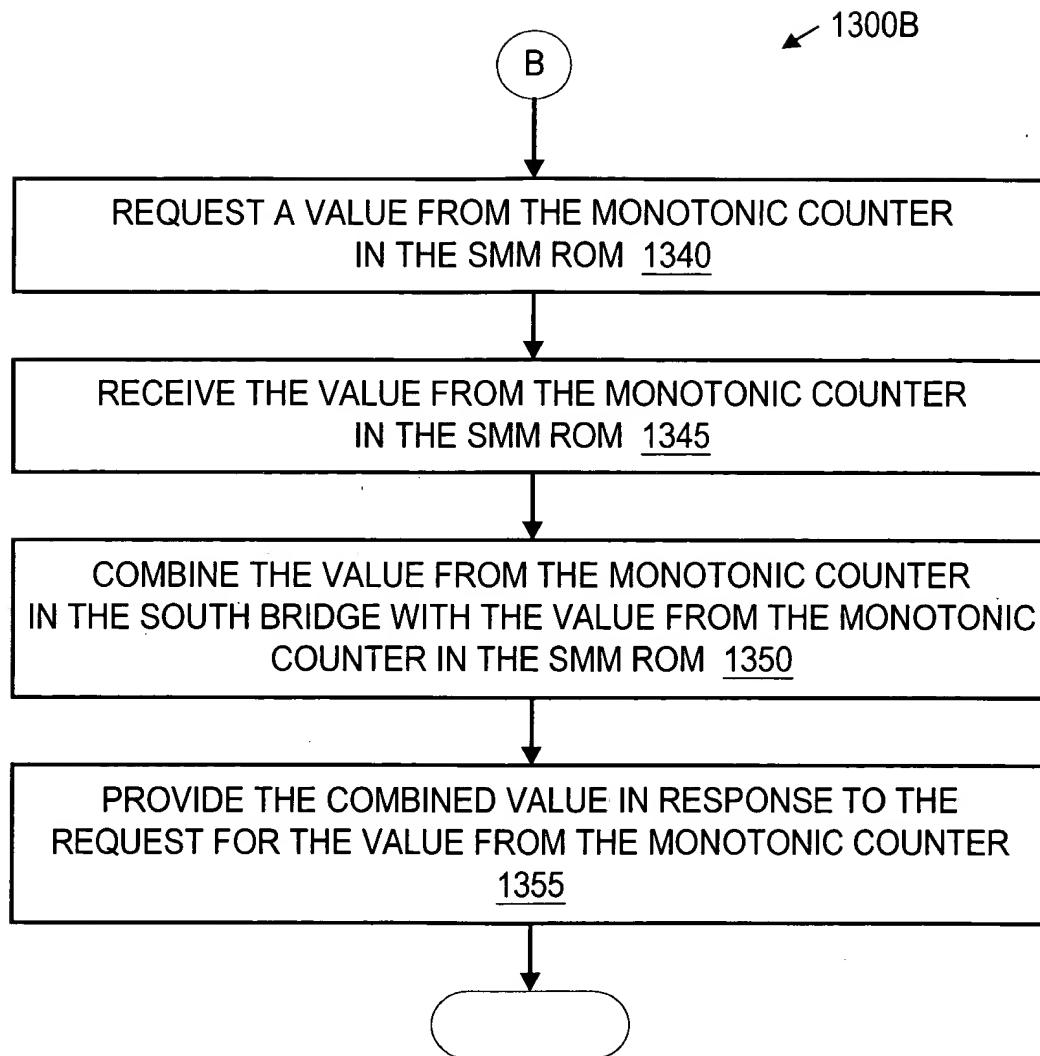


Fig. 13B

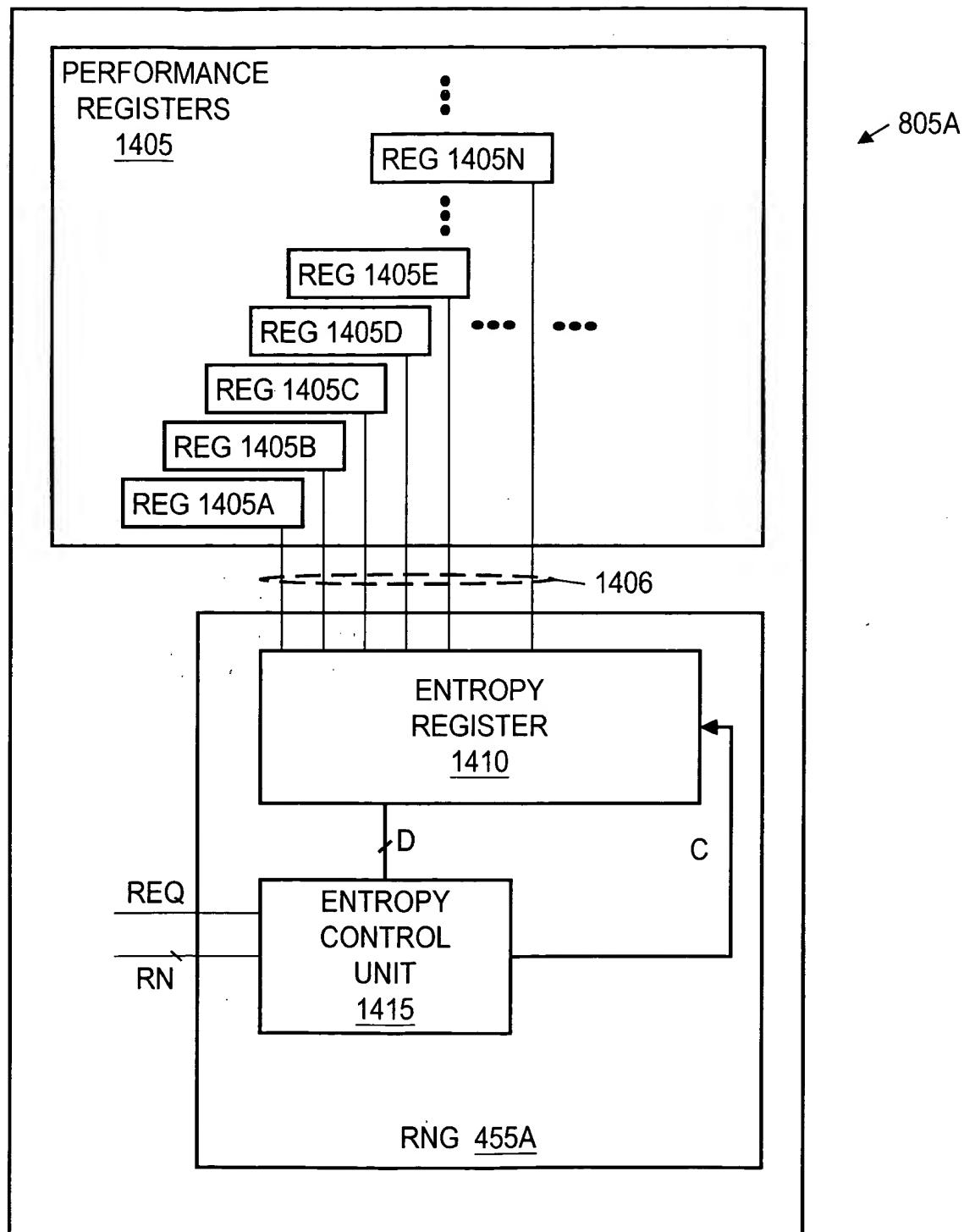


Fig. 14A

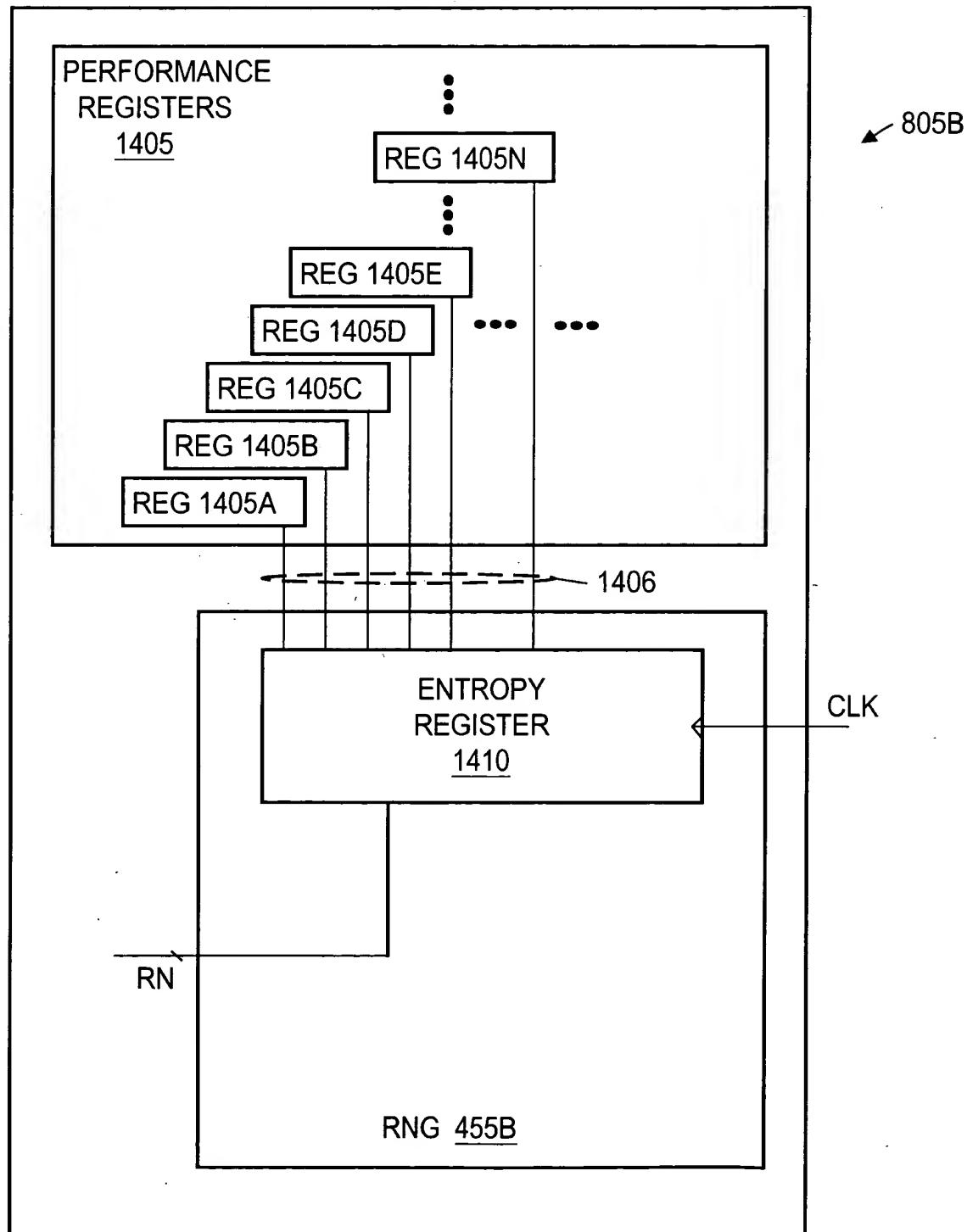
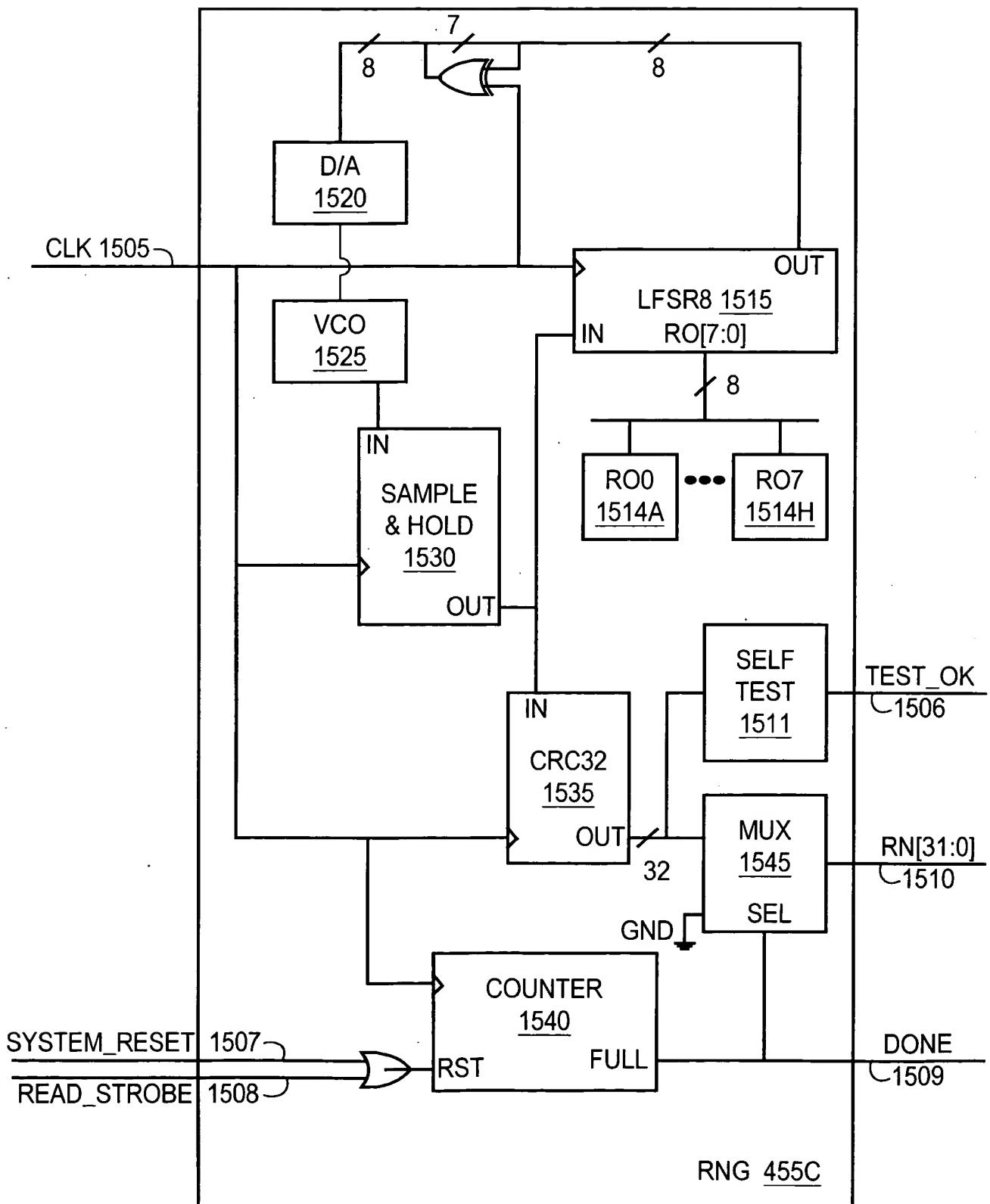


Fig. 14B

**Fig. 15**

THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620

BIOS CODE PERFORMS POWER ON SELF TEST (POST) 1625

ACCESSING THE SECURITY HARDWARE 1630

OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632

BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635

BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 1640

BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645

CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

BIOS CODE IDENTIFIES THE BOOT LOCATION 1655

BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16A

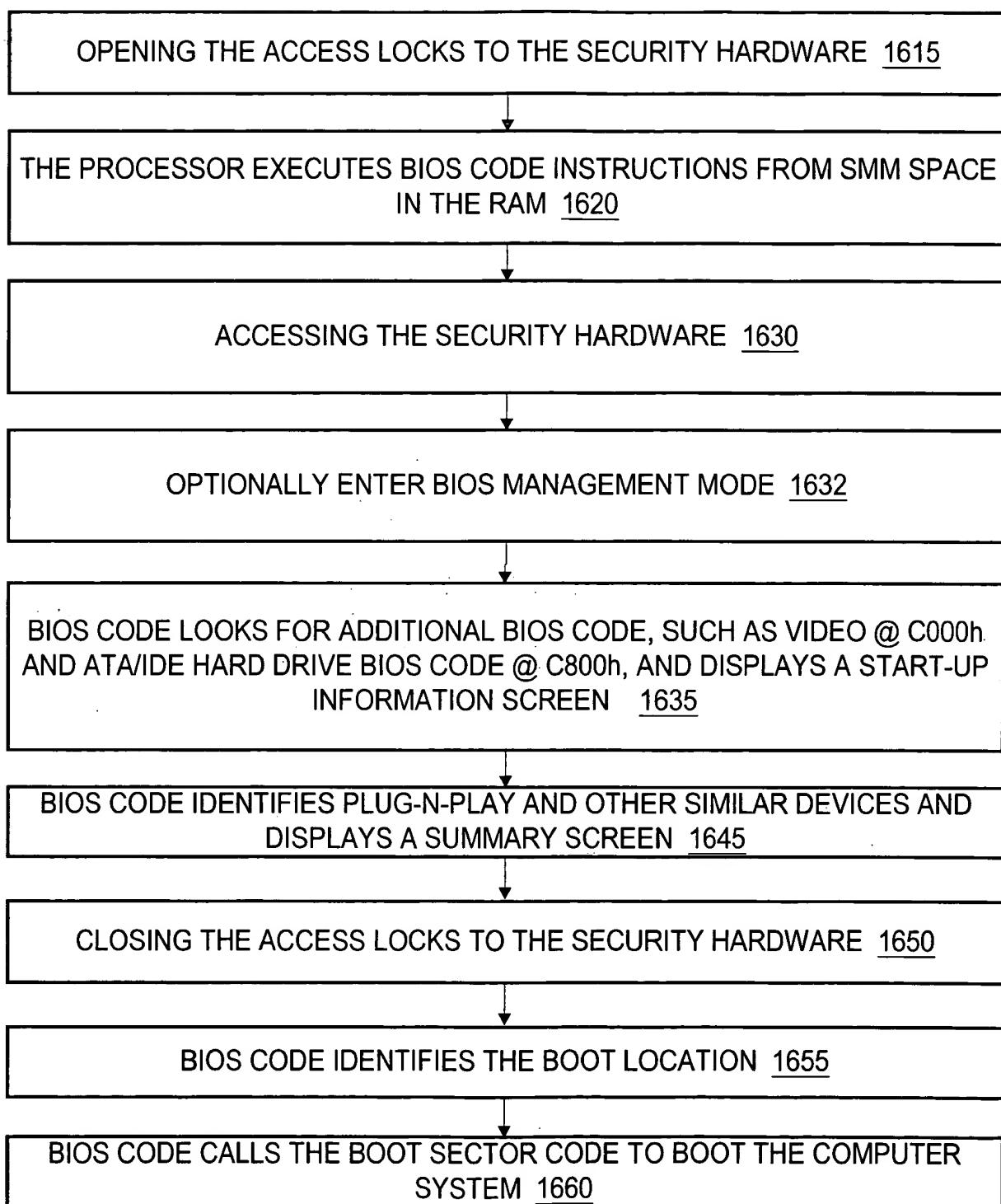


Fig. 16B

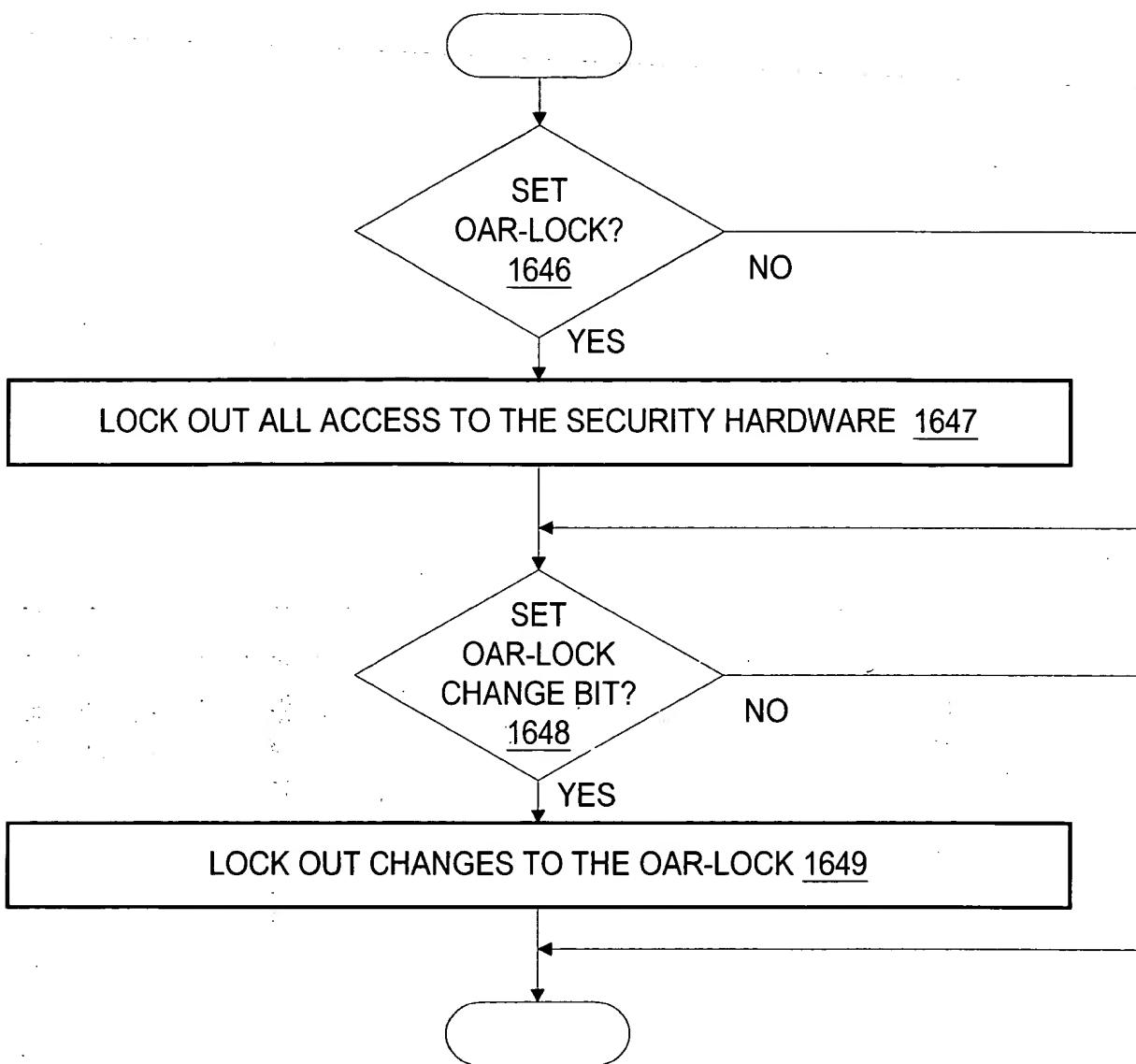


Fig. 16C

1600D

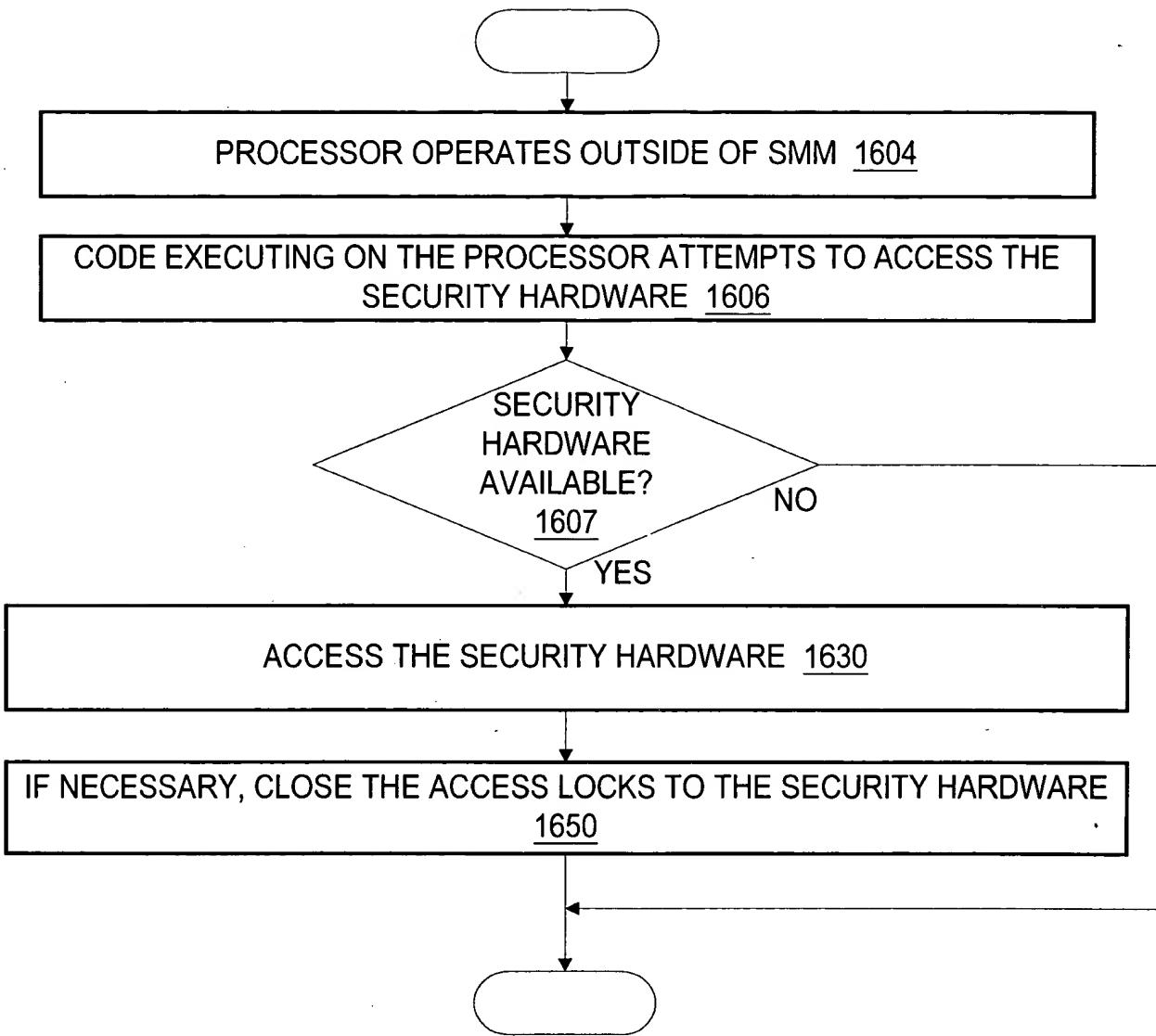


Fig. 16D

32 / 73

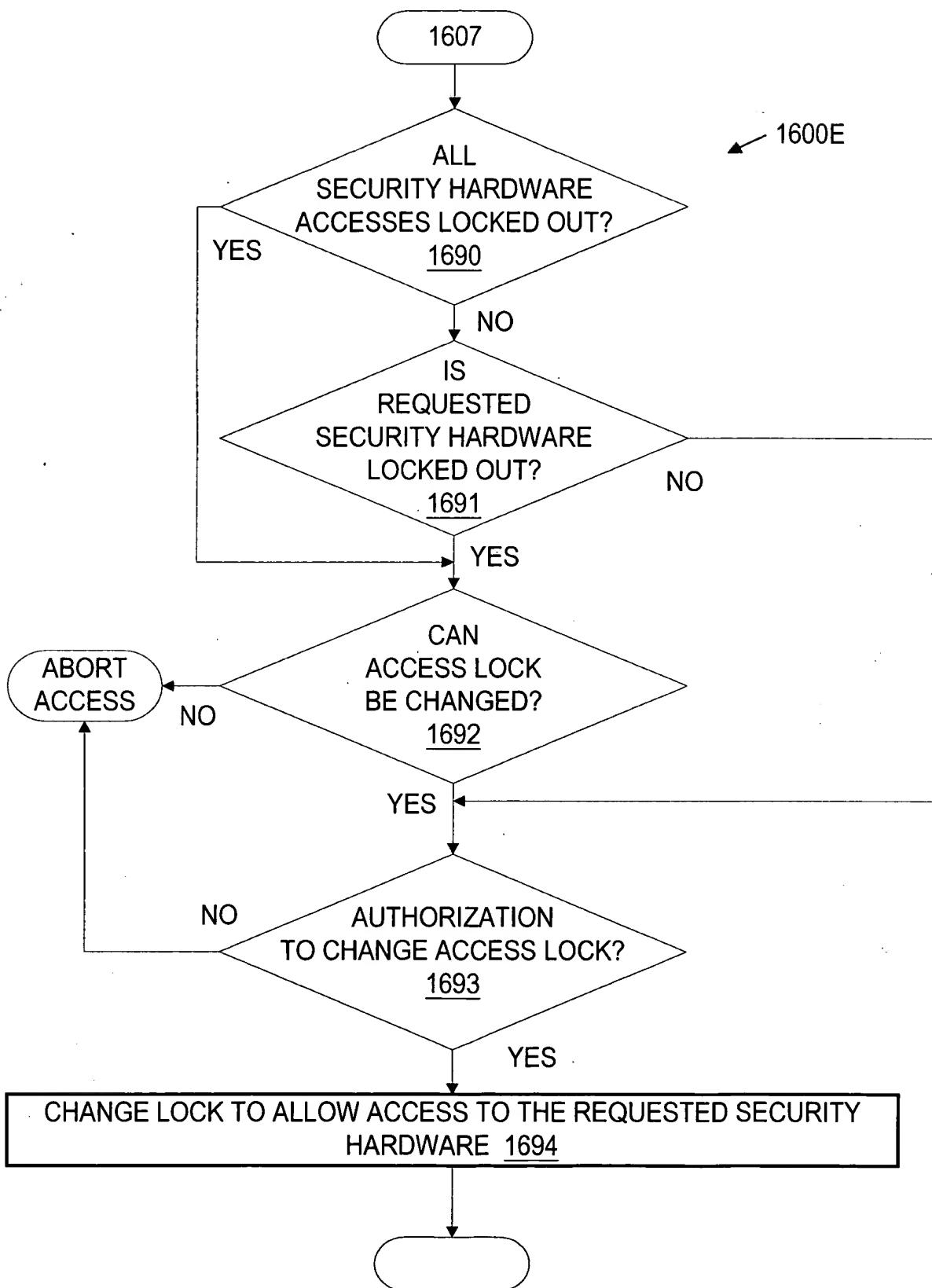


Fig. 16E

1600F

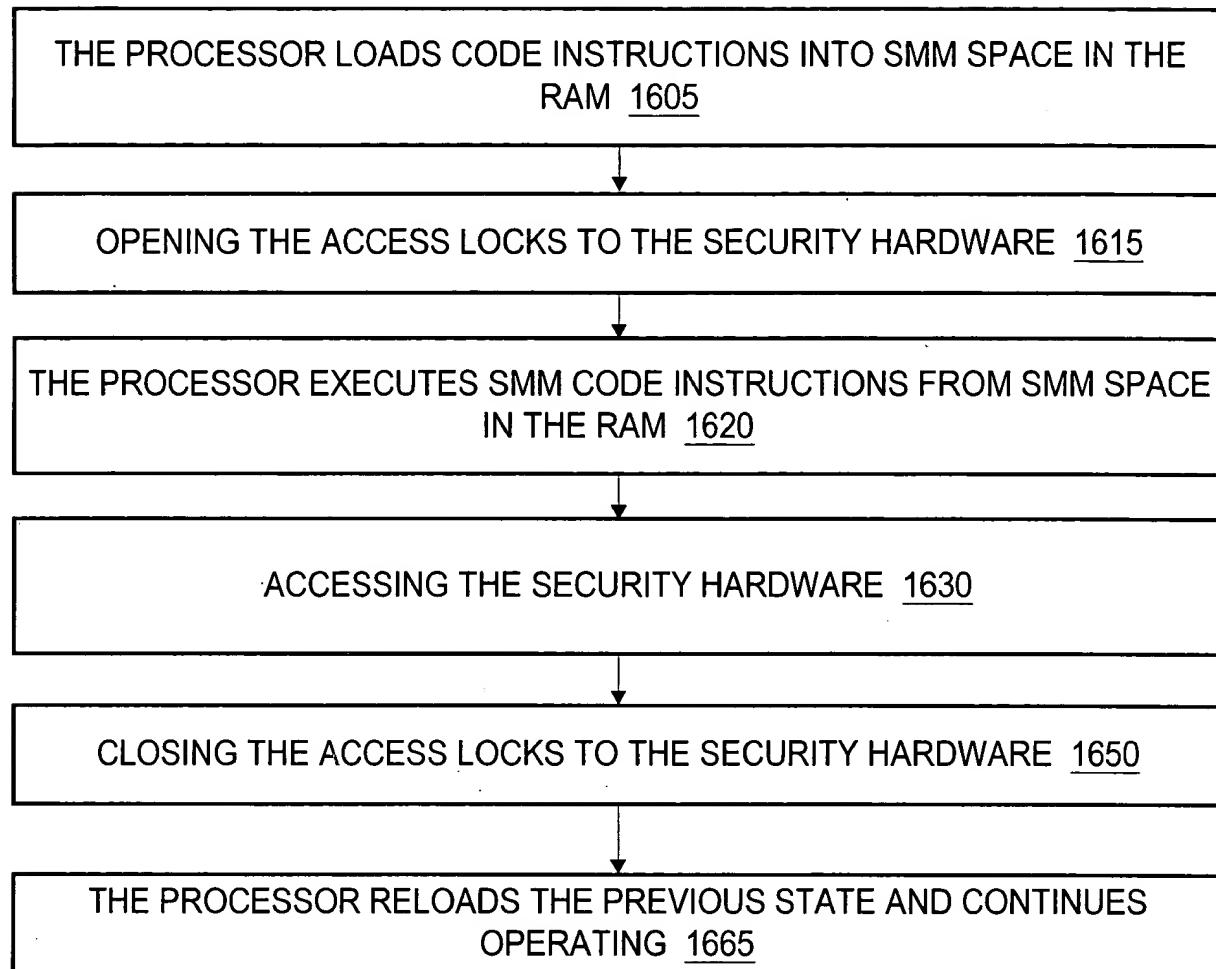


Fig. 16F

1600G

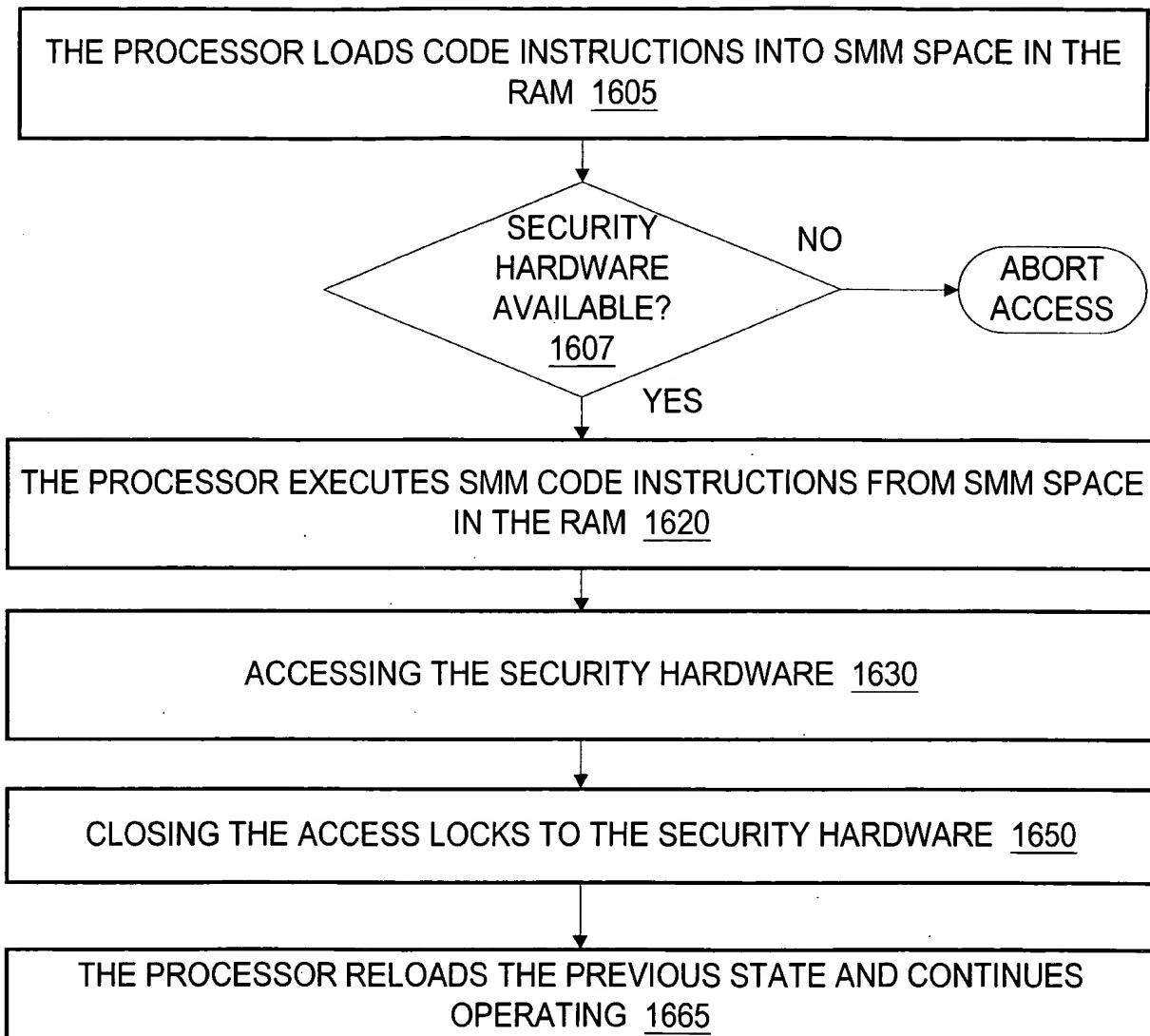


Fig. 16G

35 / 73

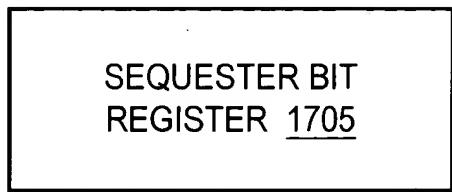


Fig. 17A



Fig. 17B

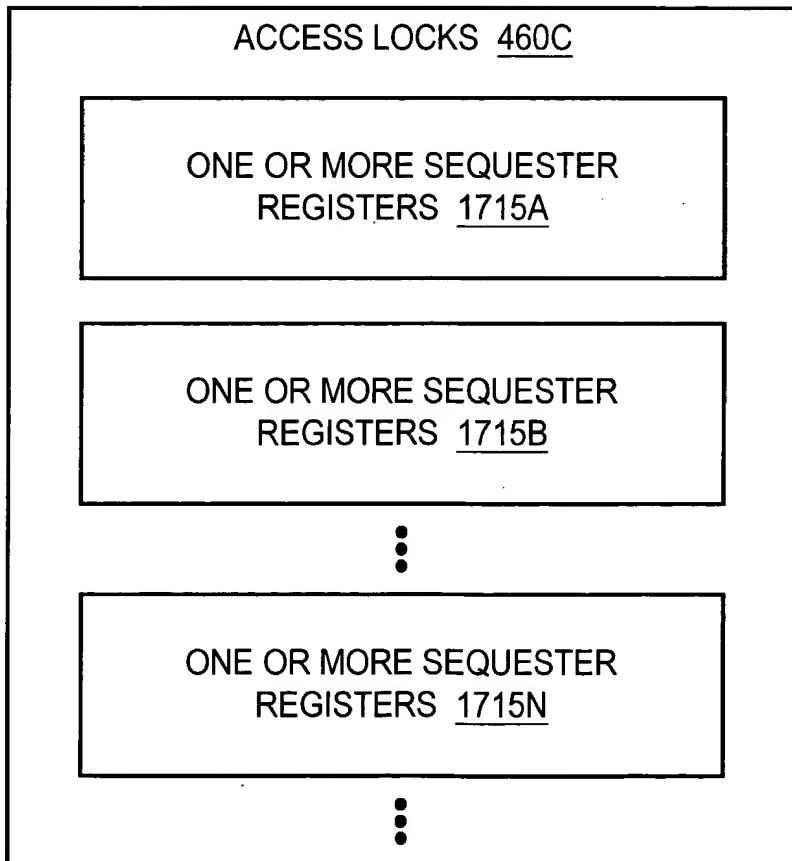


Fig. 17C

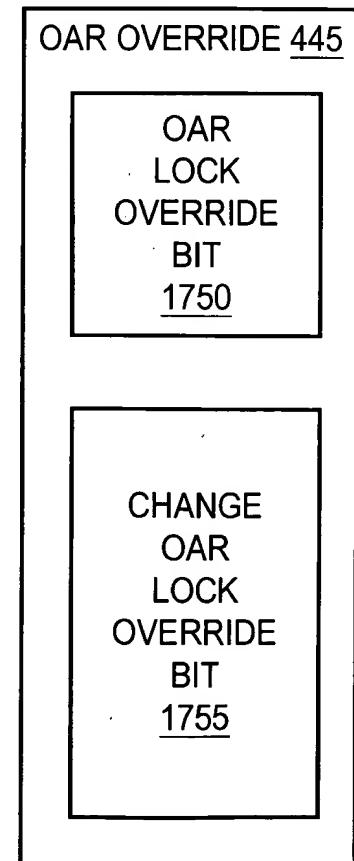


Fig. 17D

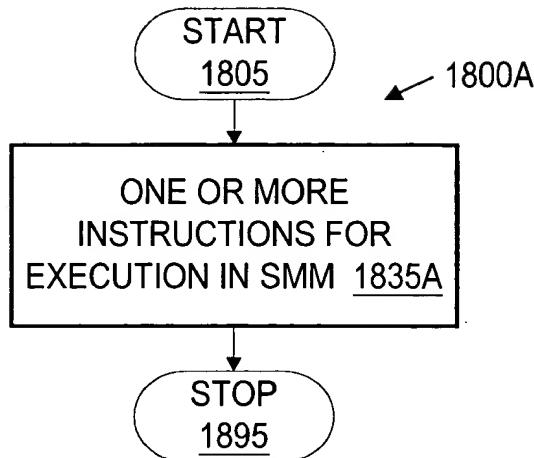


Fig. 18A
PRIOR ART

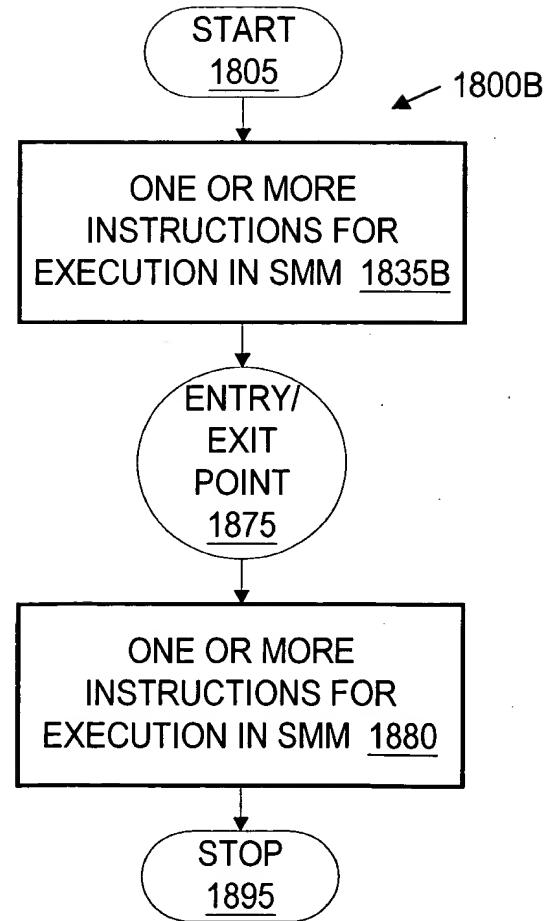


Fig. 18B

37 / 73

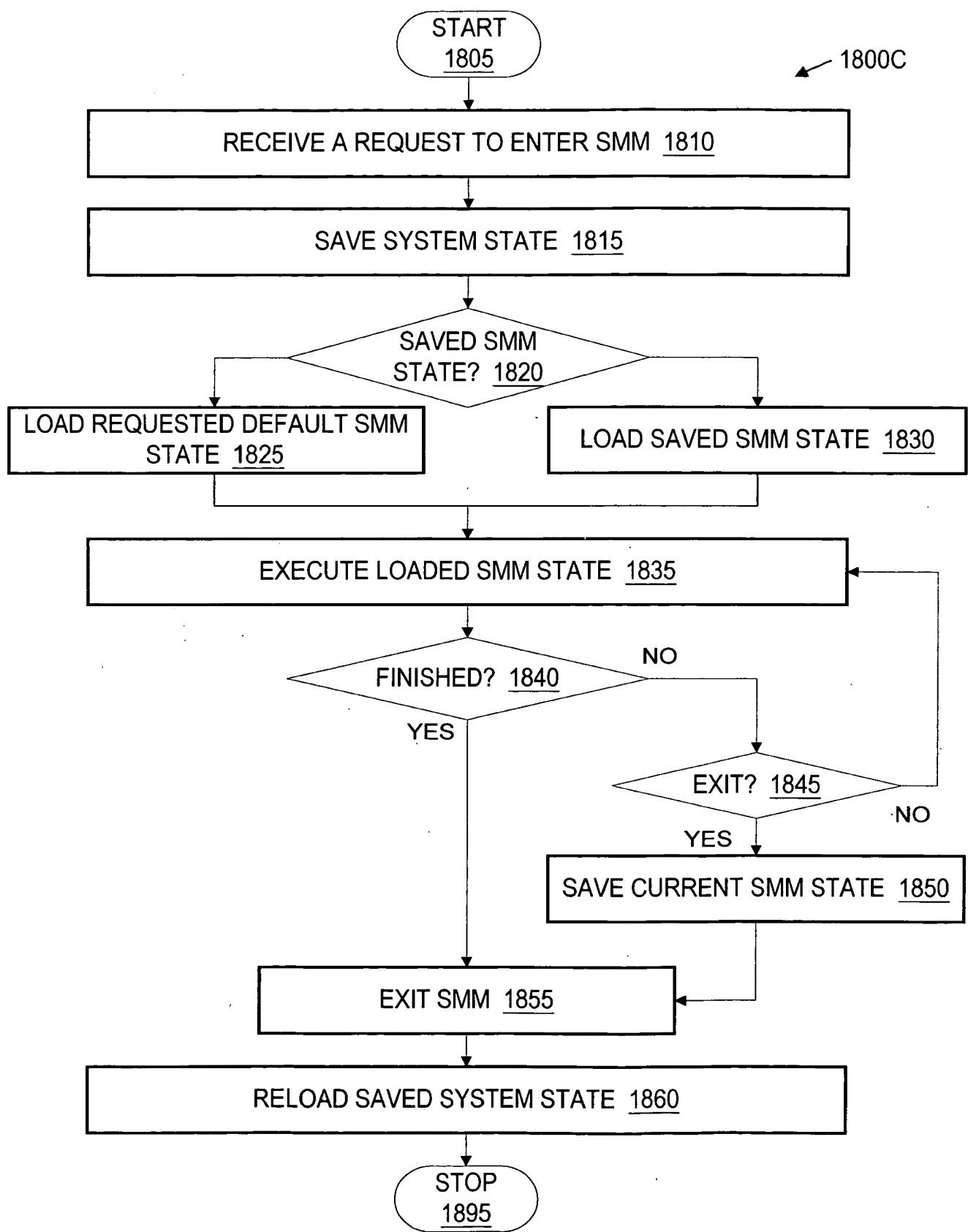


Fig. 18C

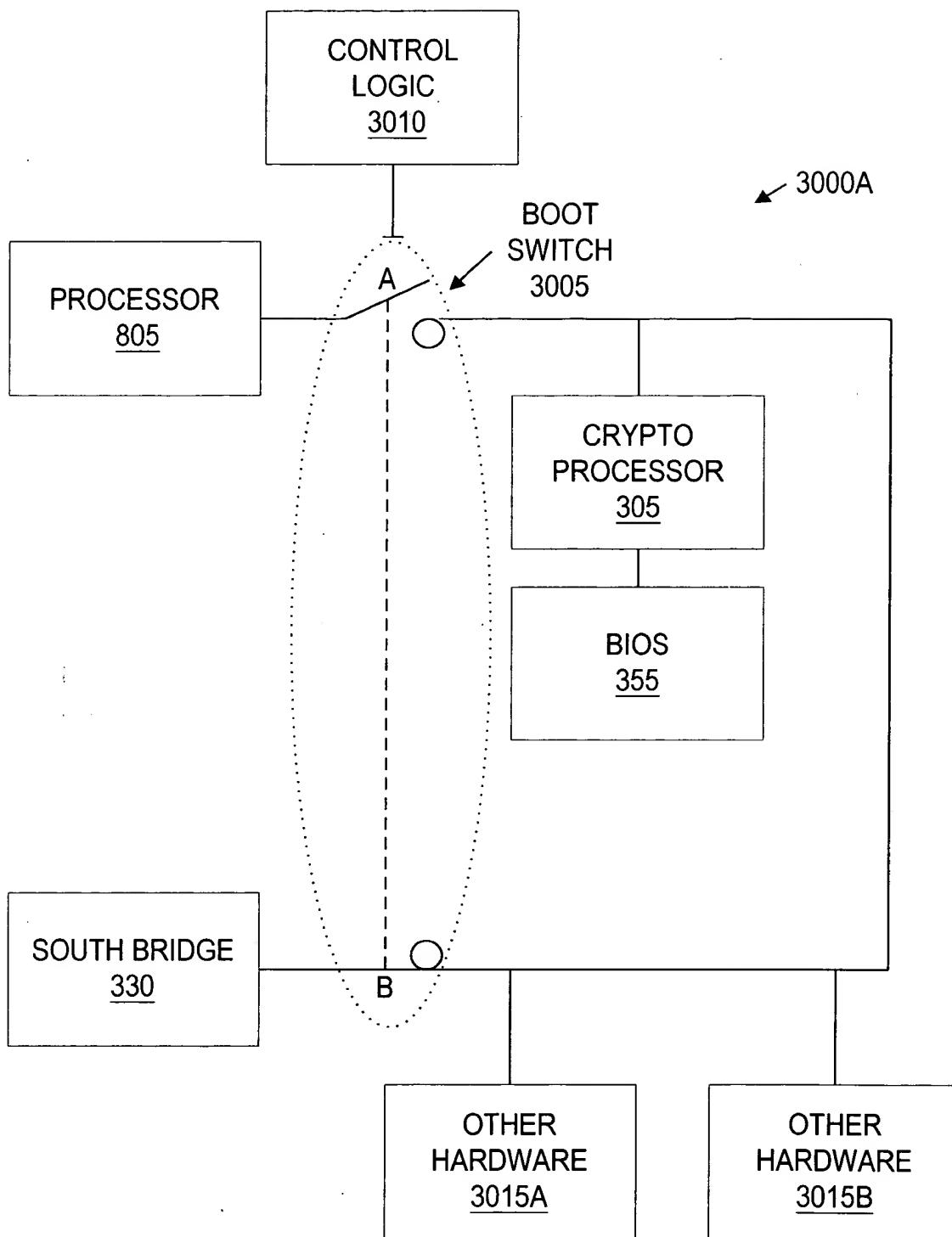
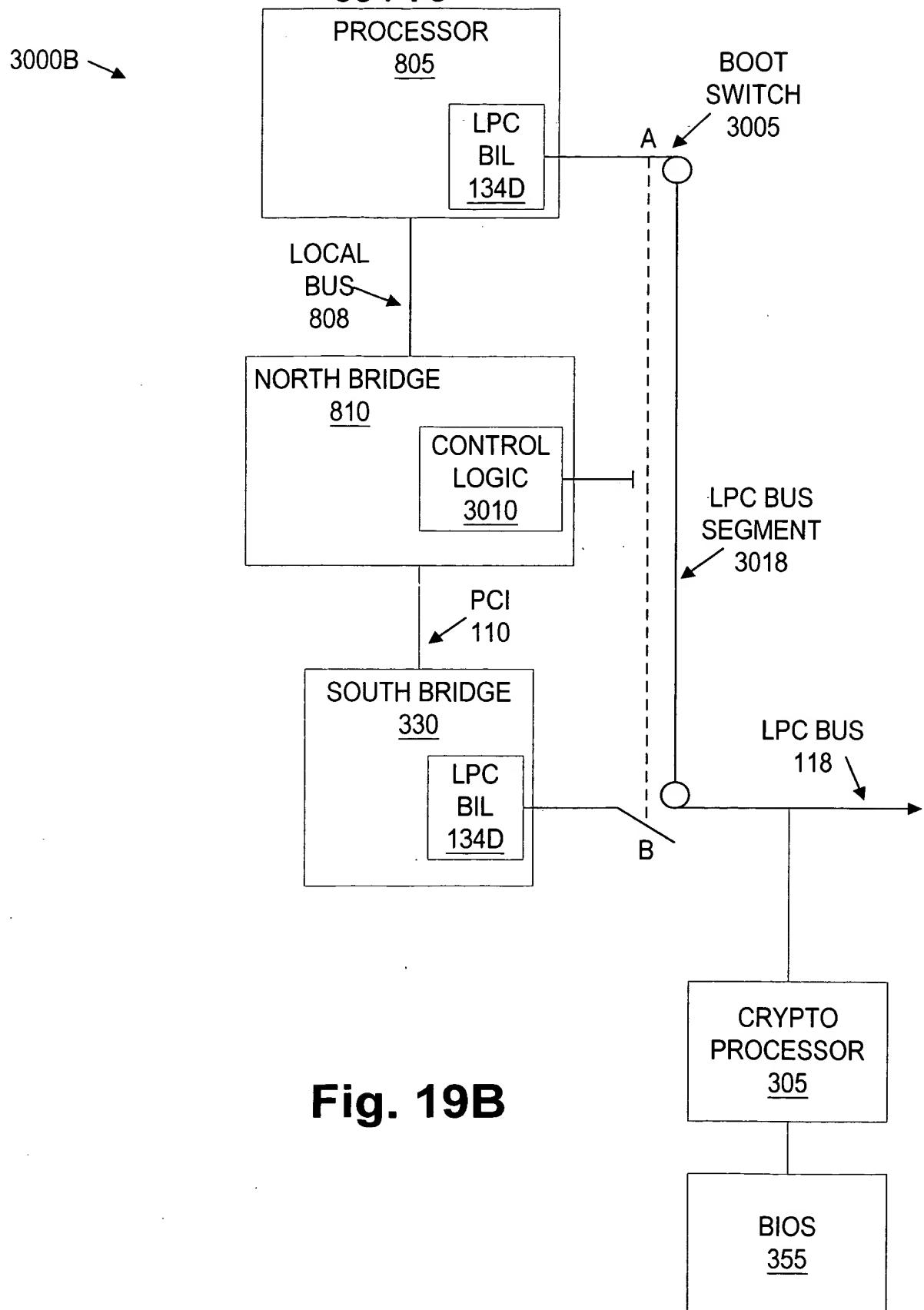


Fig. 19A

39 / 73



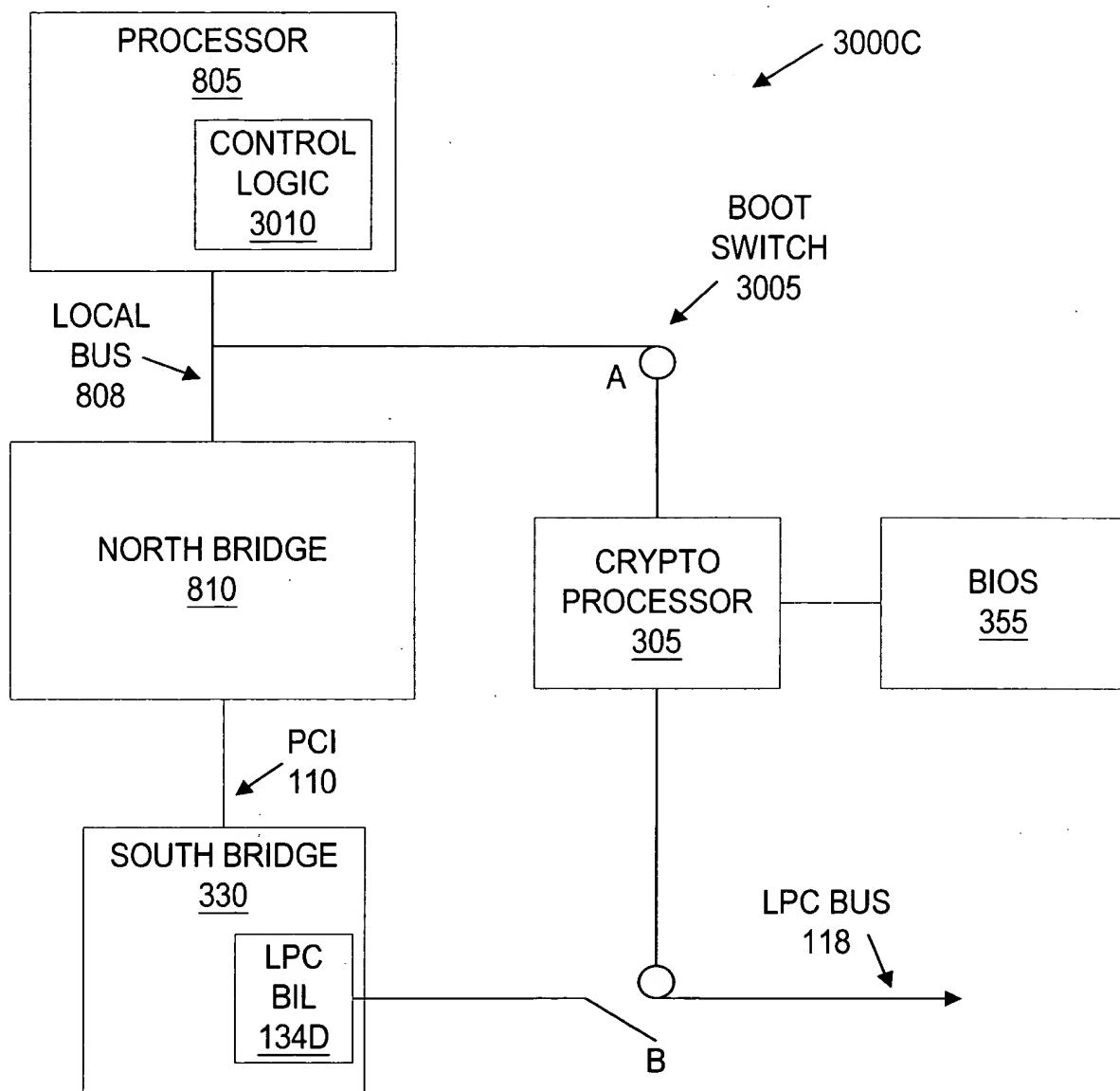


Fig. 19C

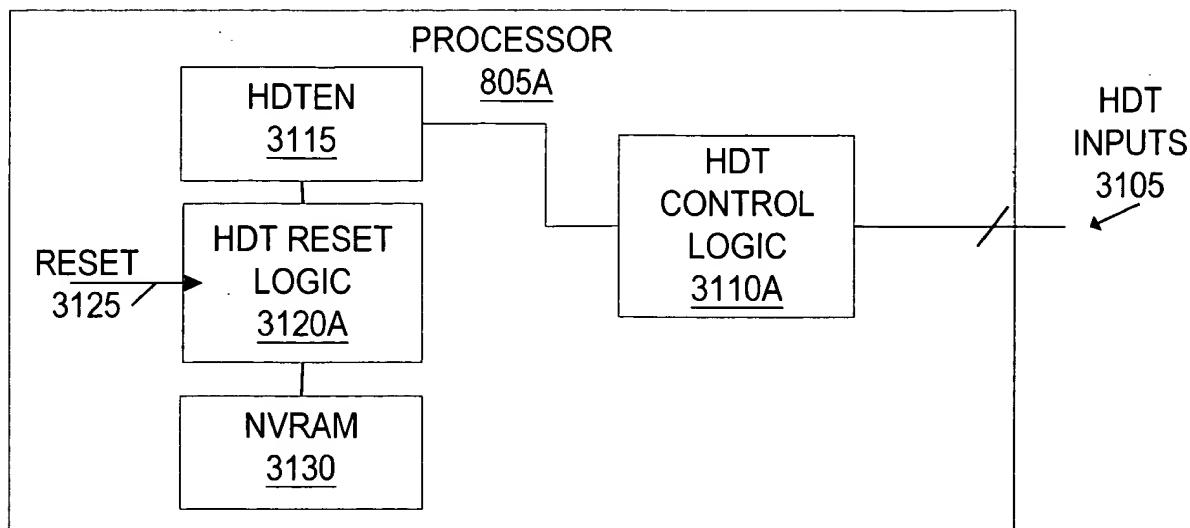


Fig. 20A

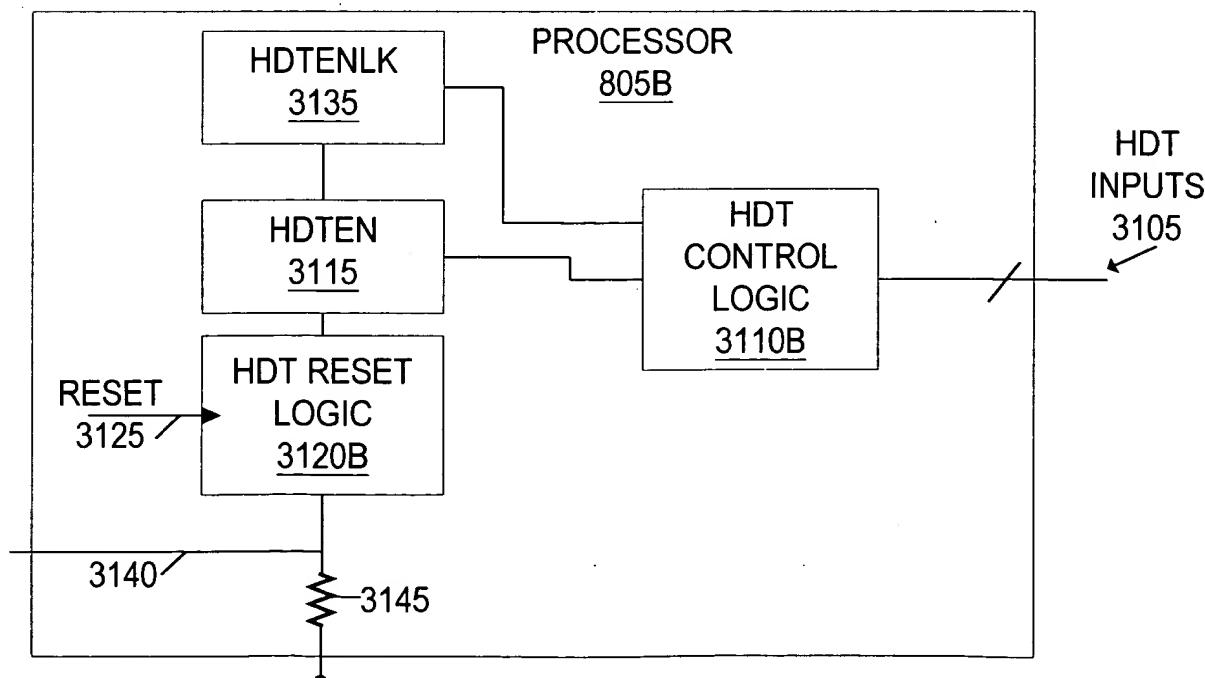
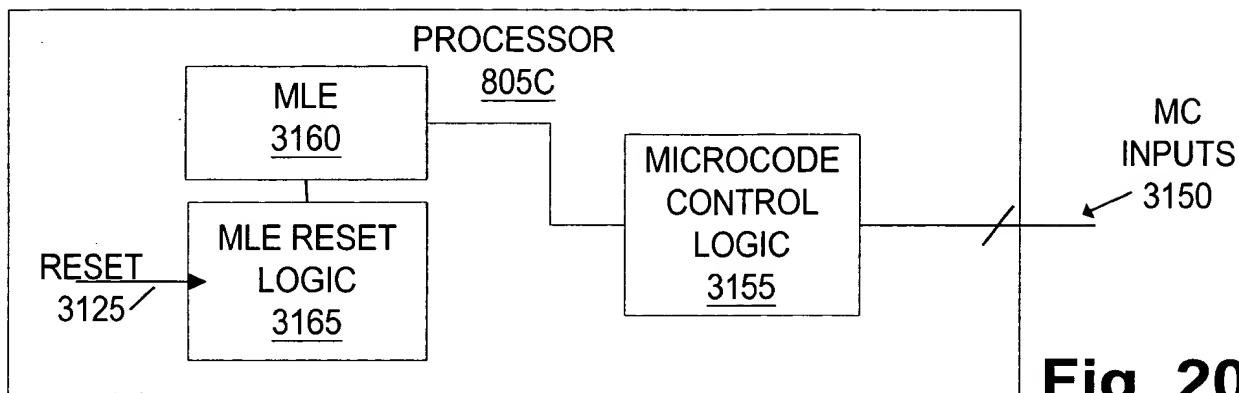
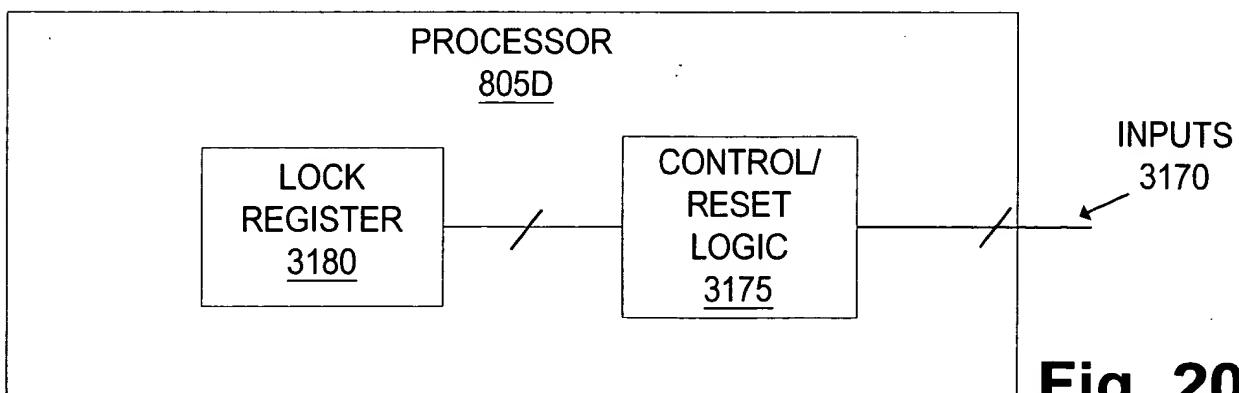
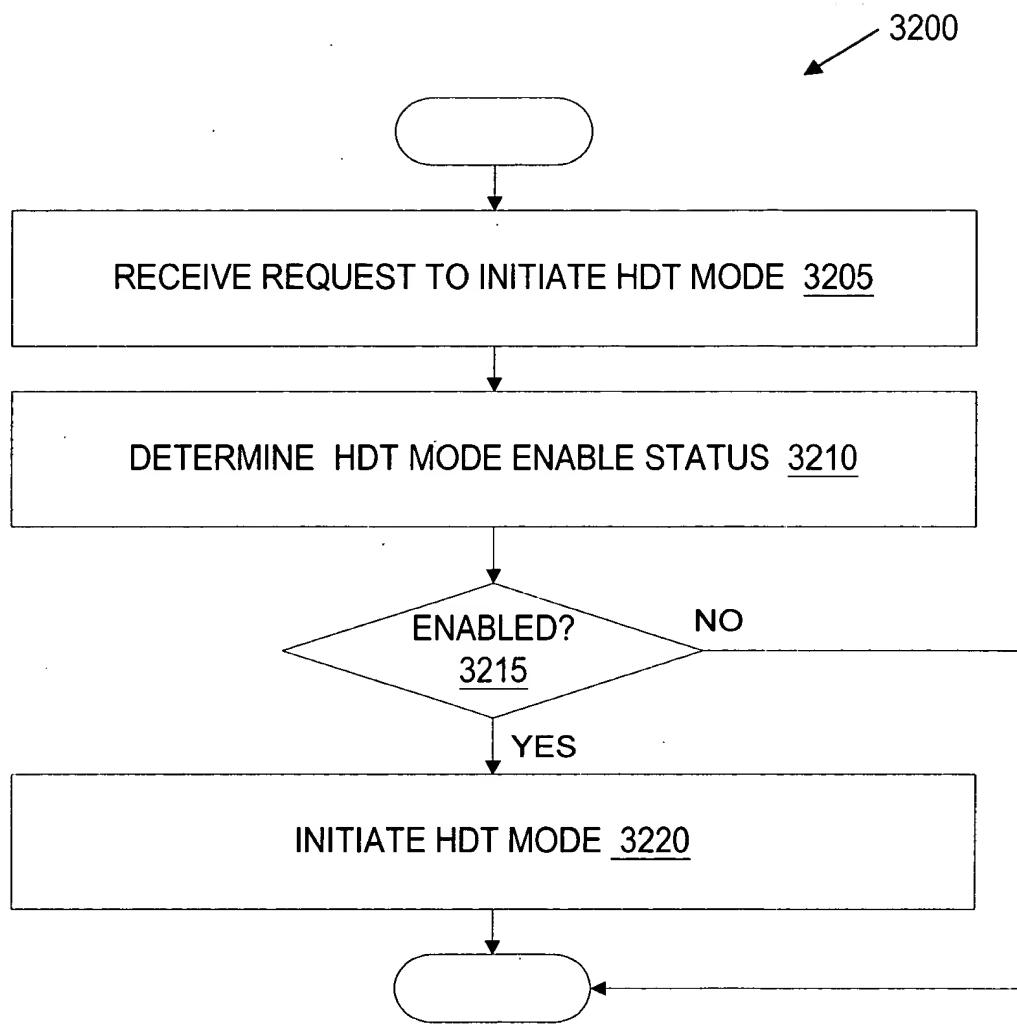


Fig. 20B

**Fig. 20C****Fig. 20D**

**Fig. 21**

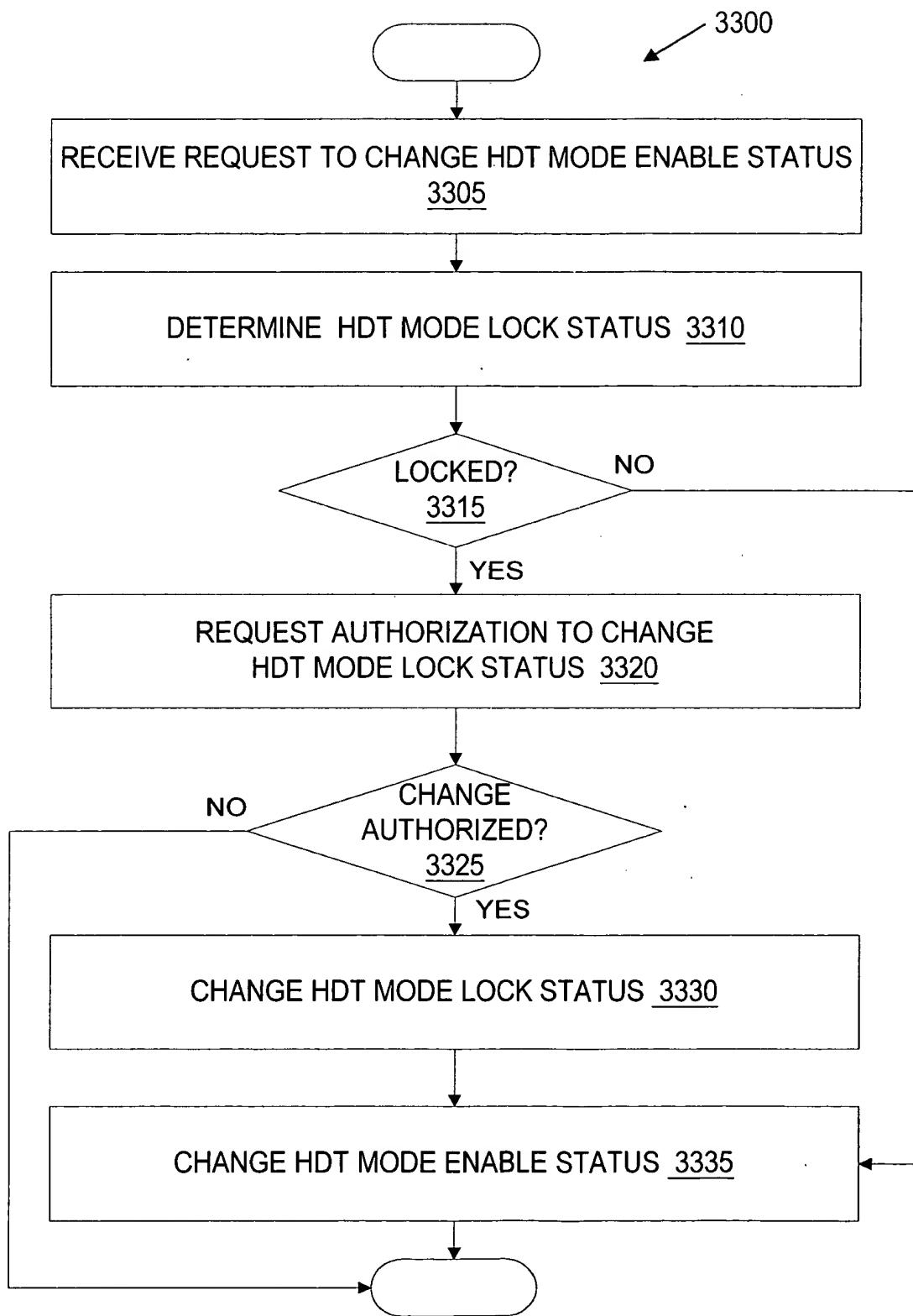
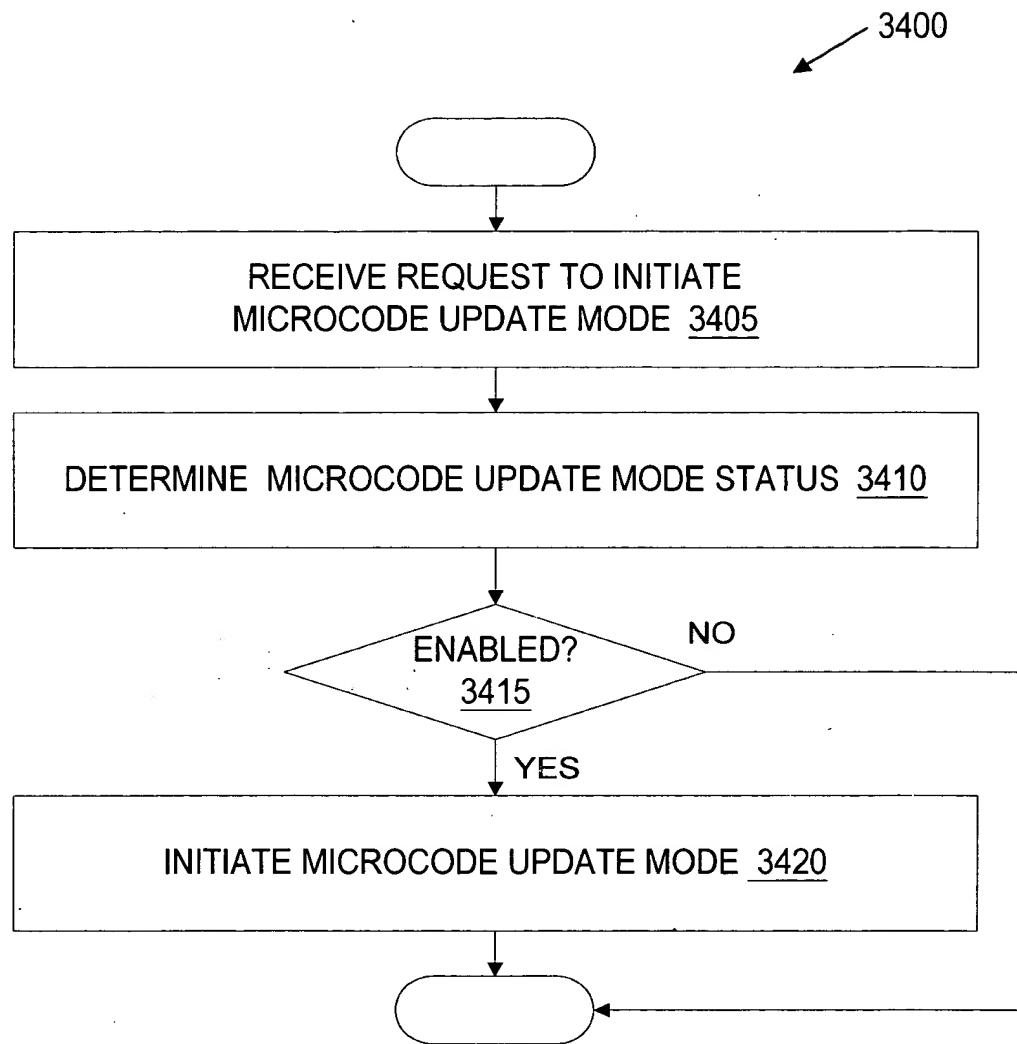


Fig. 22

**Fig. 23**

46 / 73

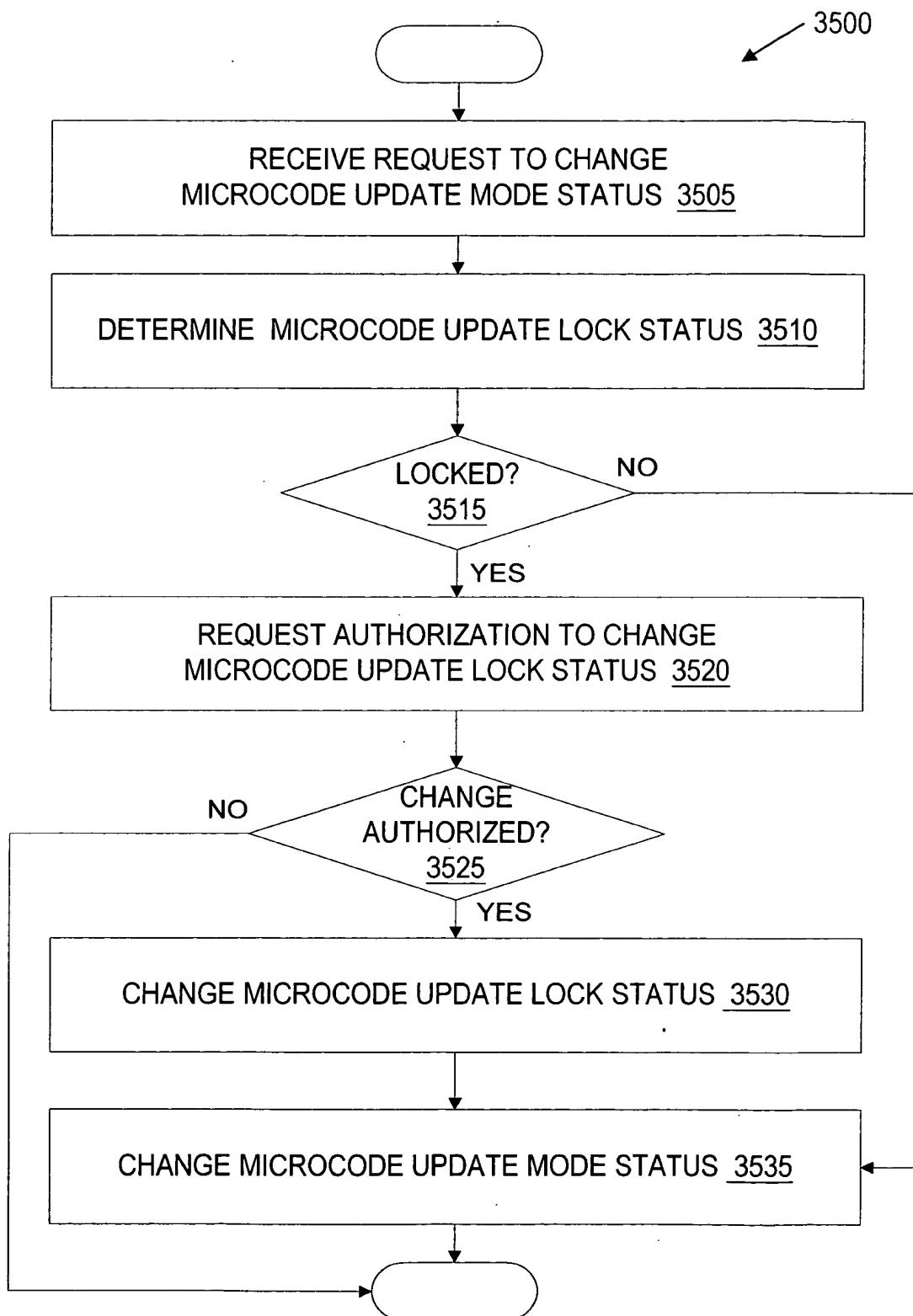


Fig. 24

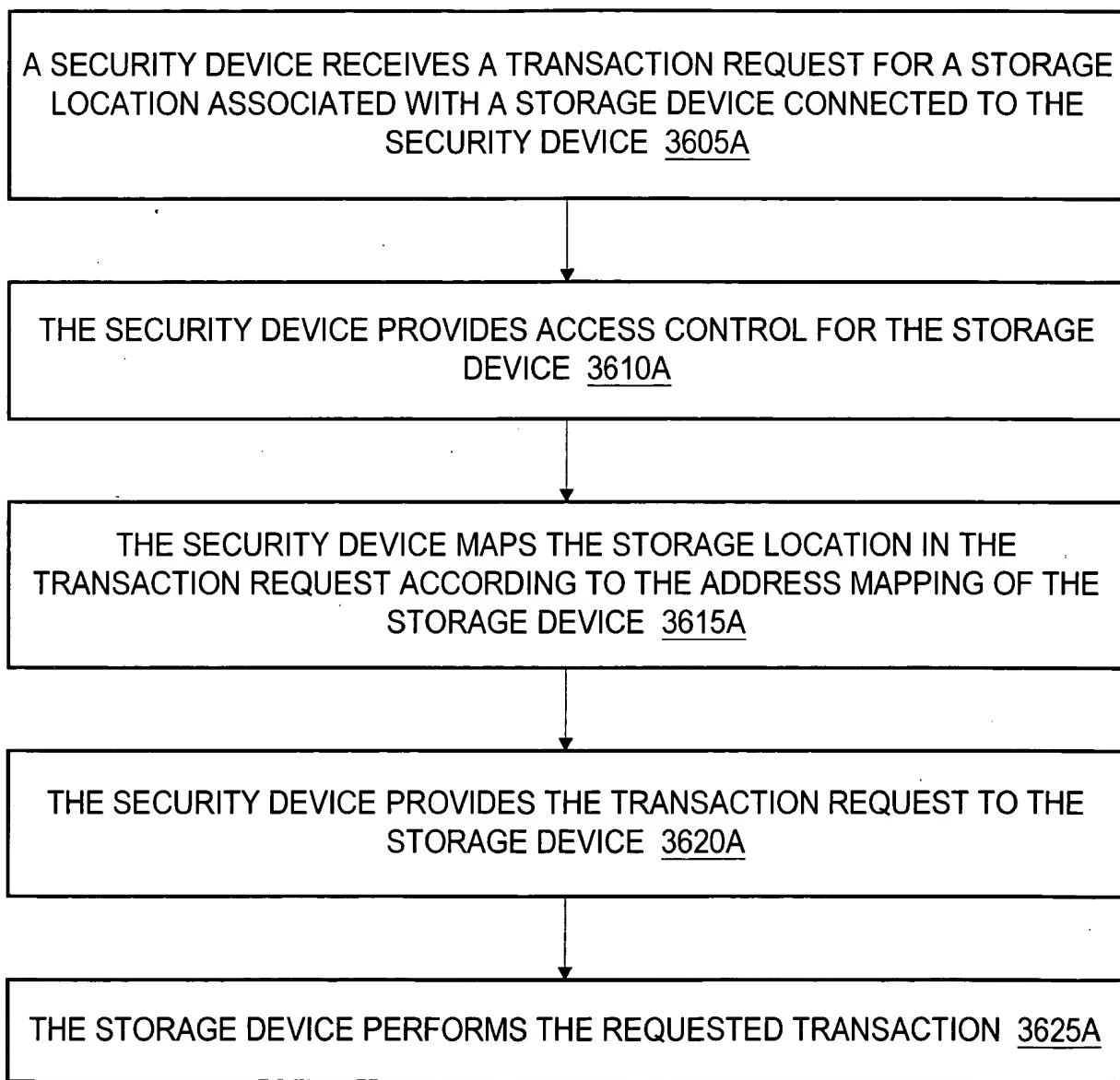


Fig. 25A

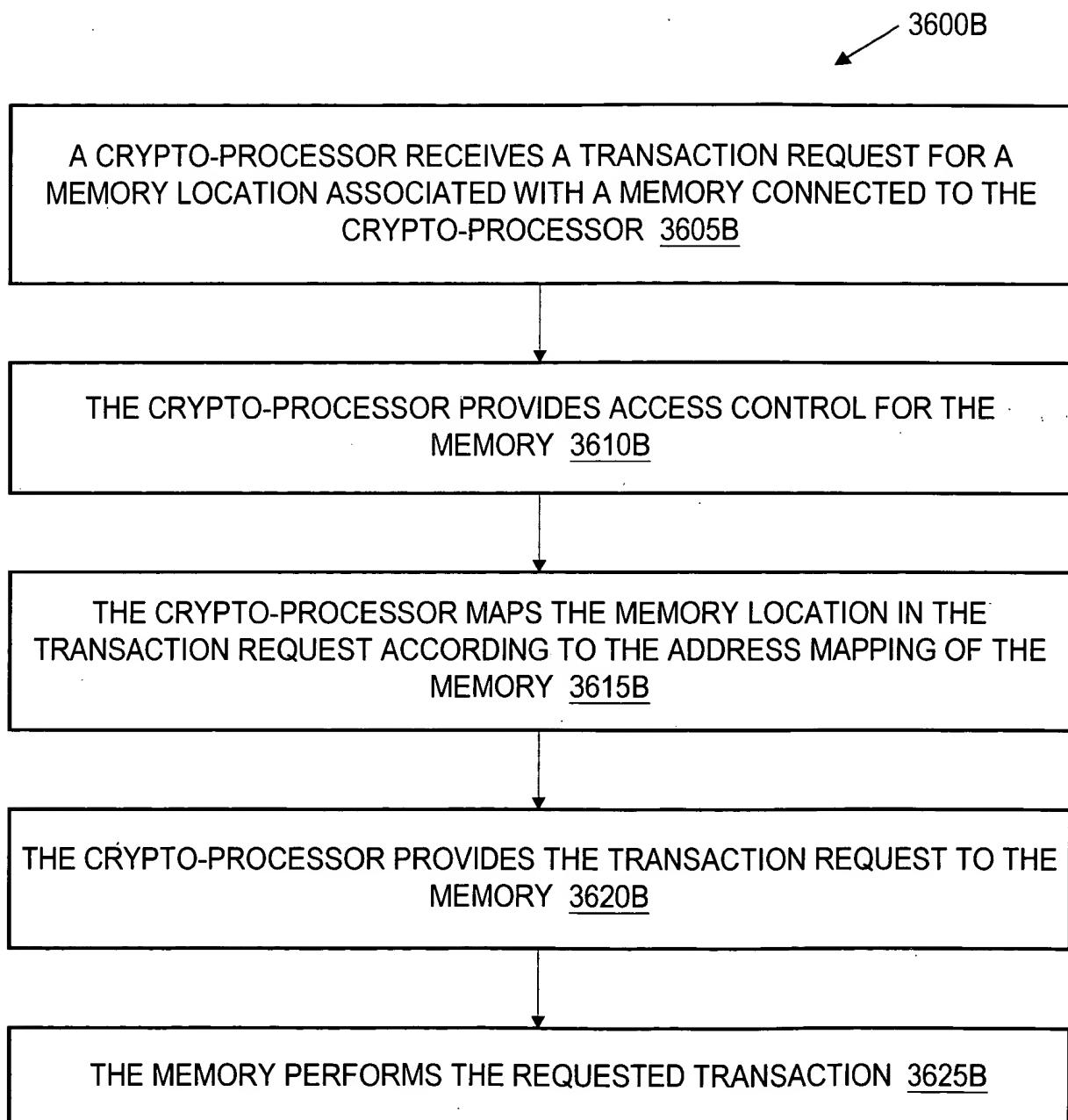


Fig. 25B

3610A

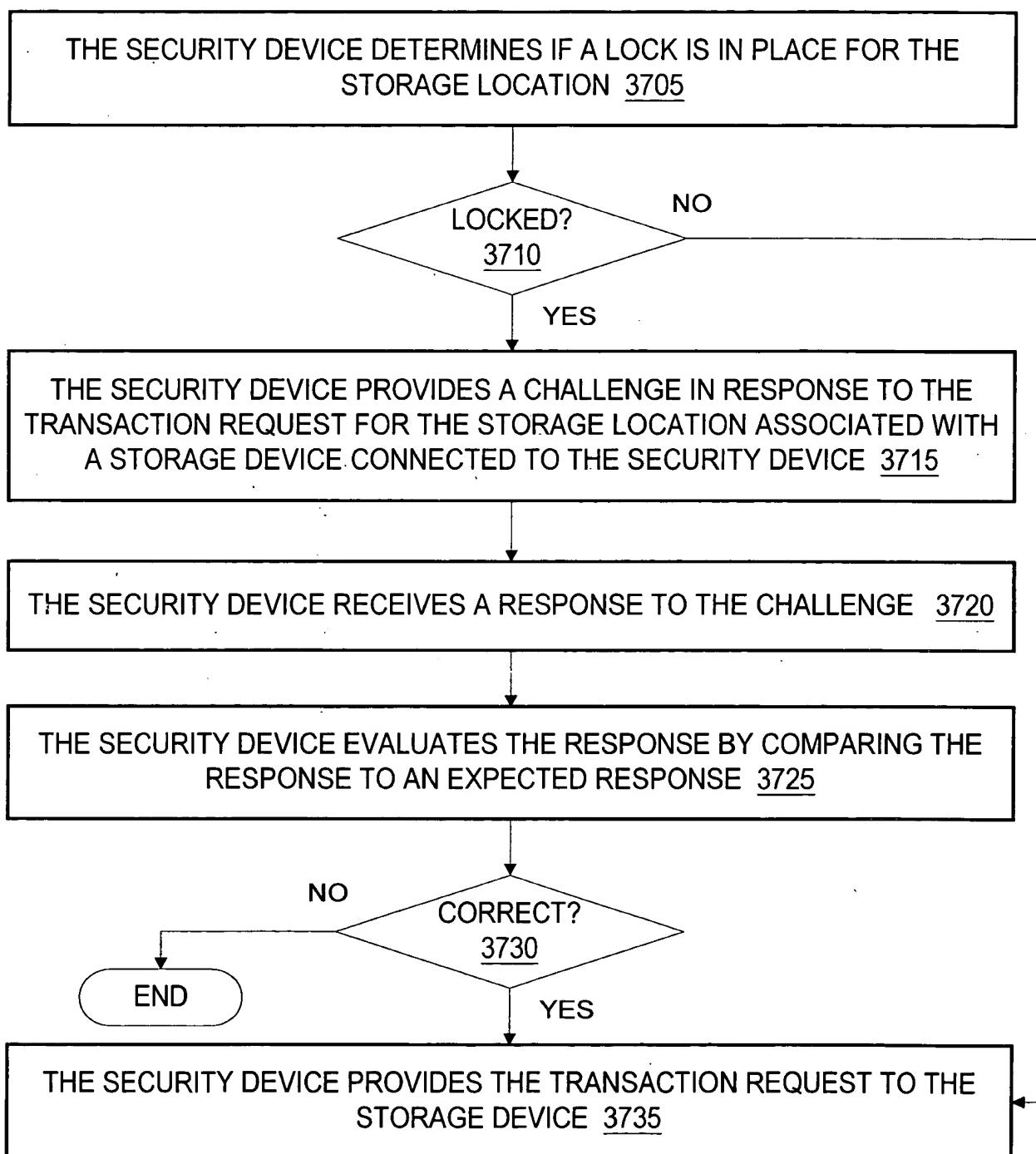


Fig. 26

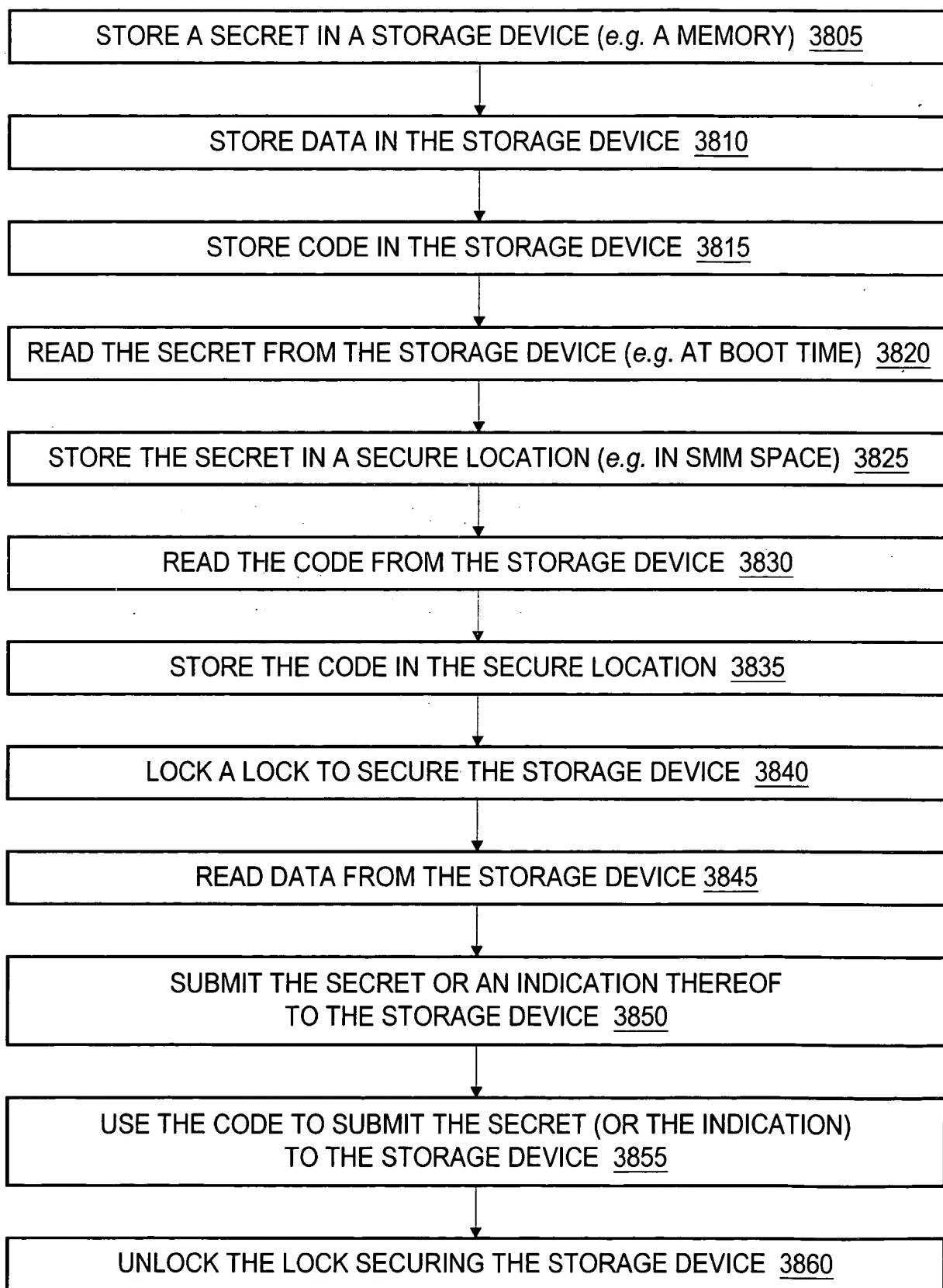


Fig. 27

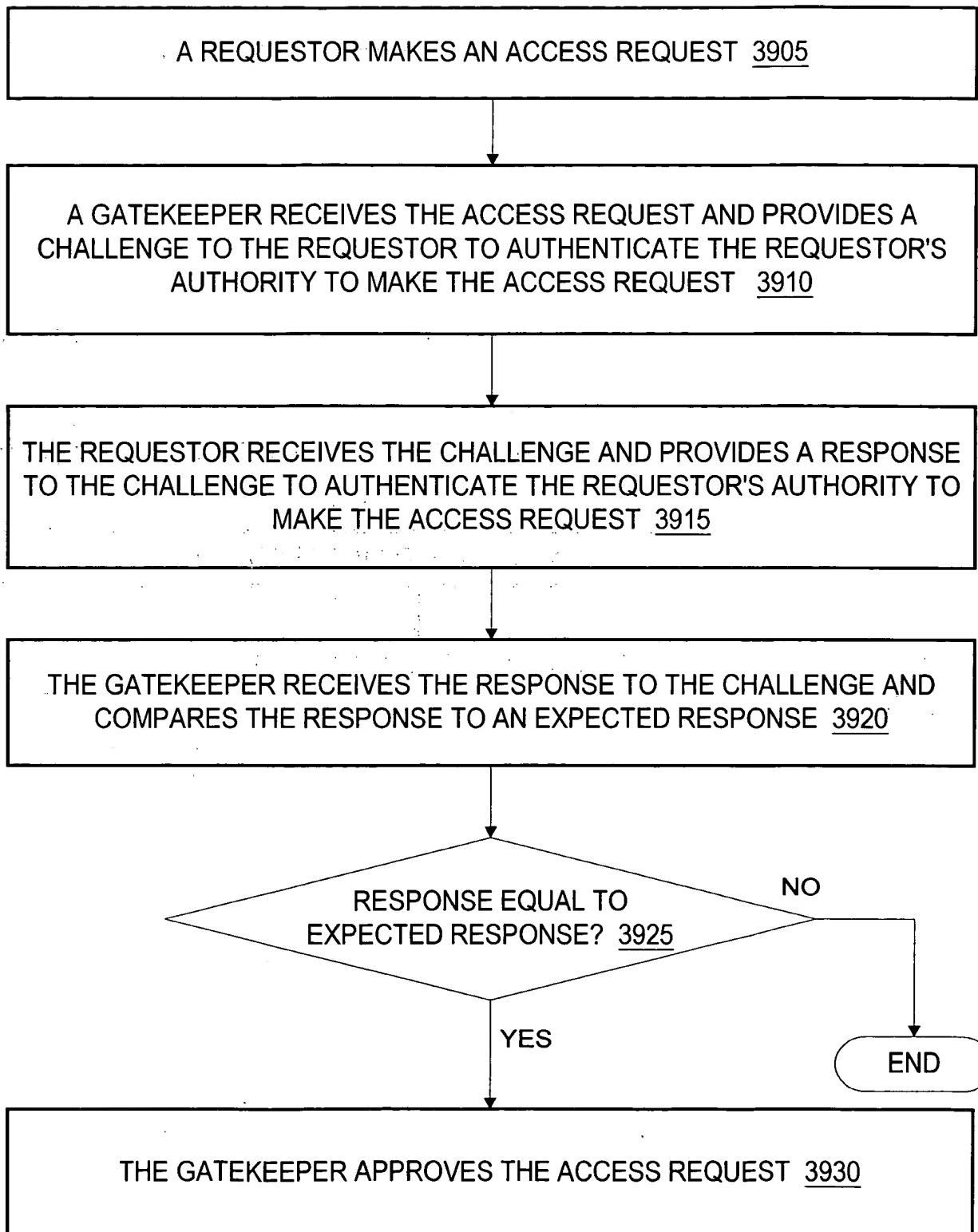


Fig. 28
(Prior Art)

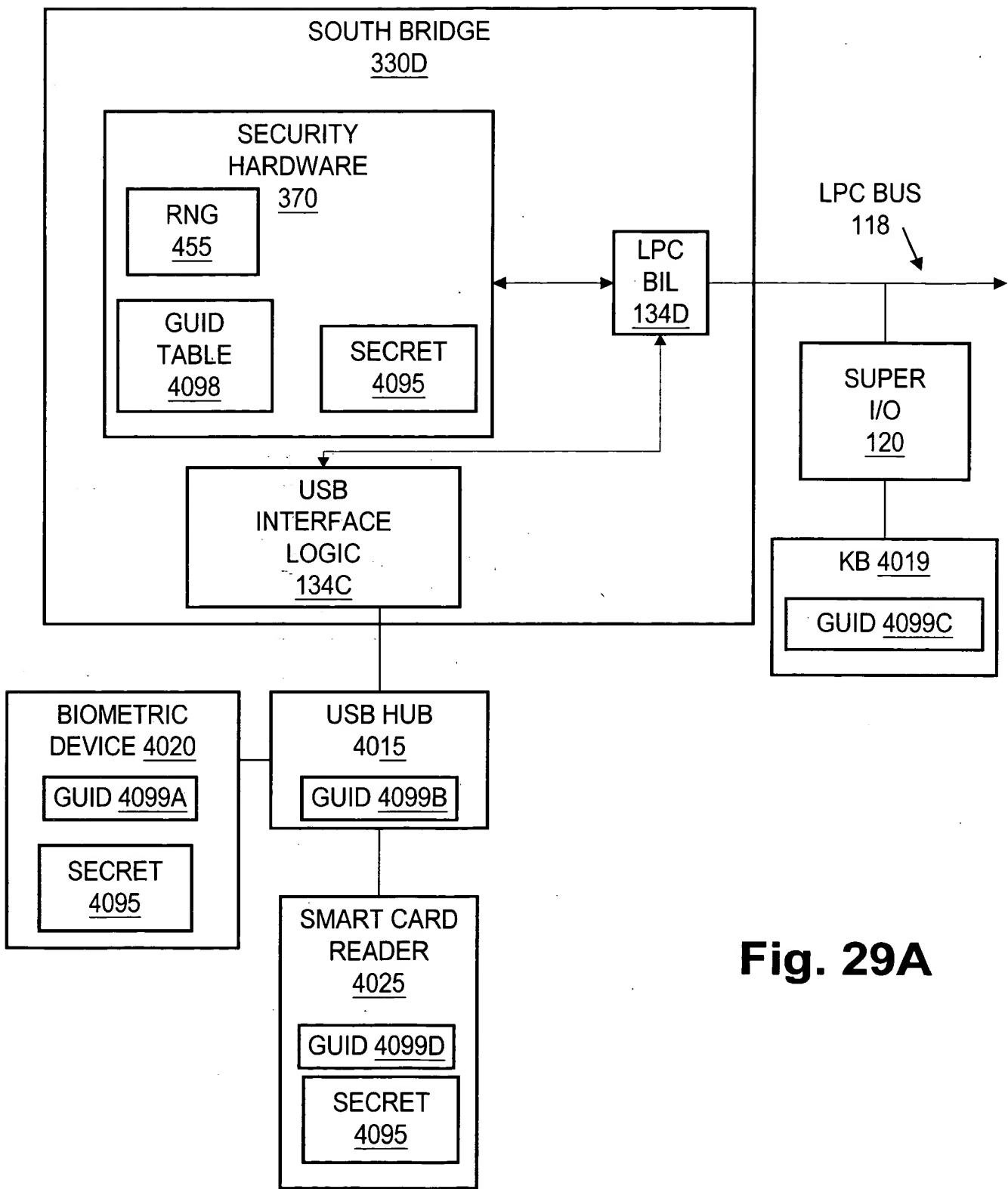


Fig. 29A

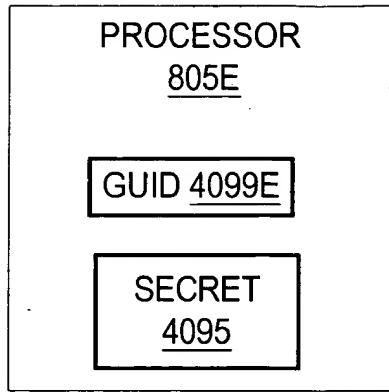


Fig. 29B

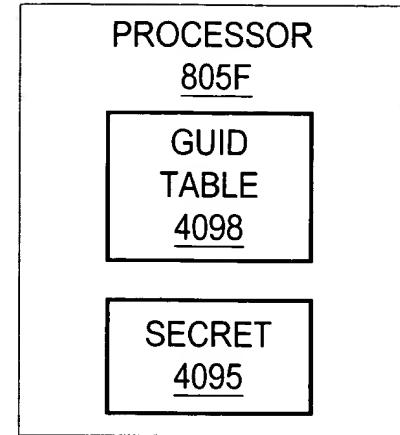
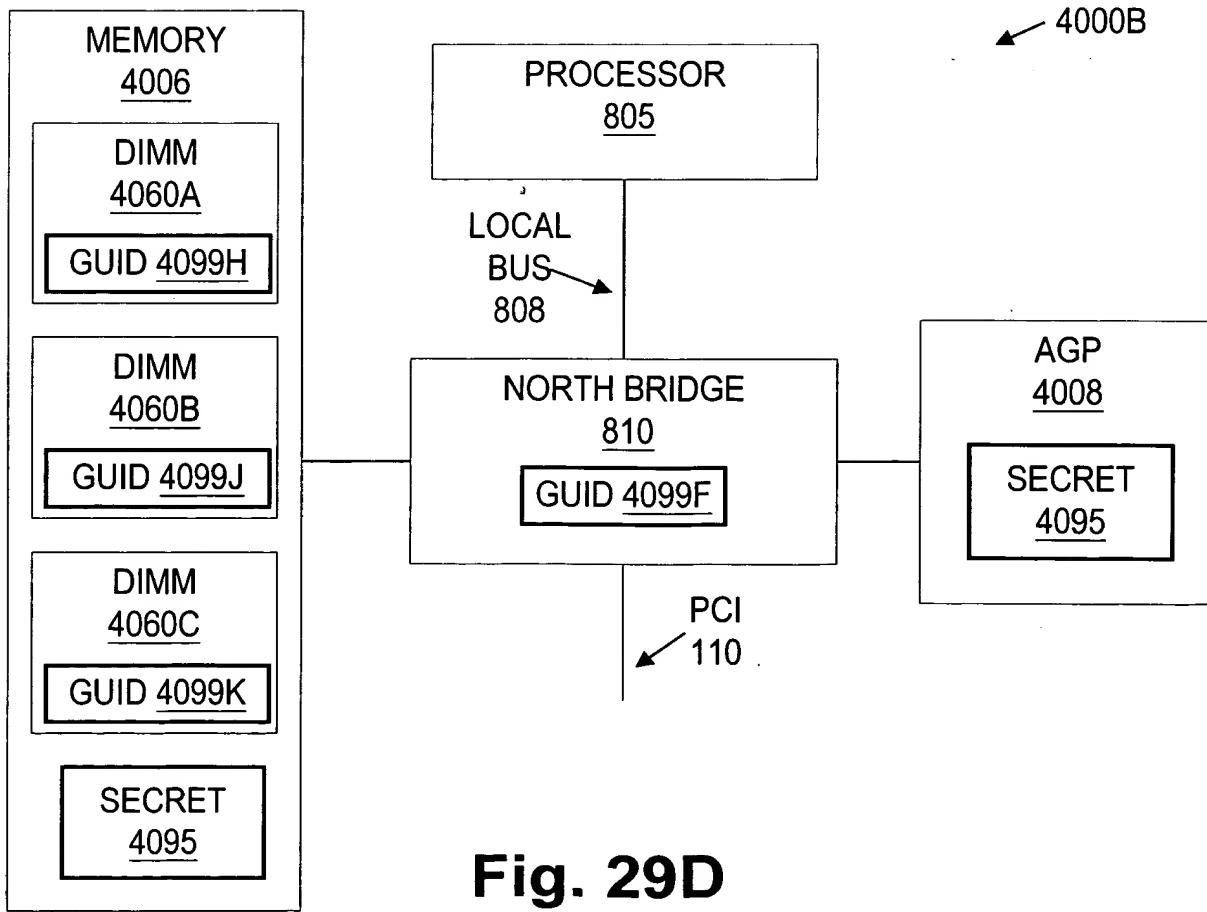


Fig. 29C



54 / 73

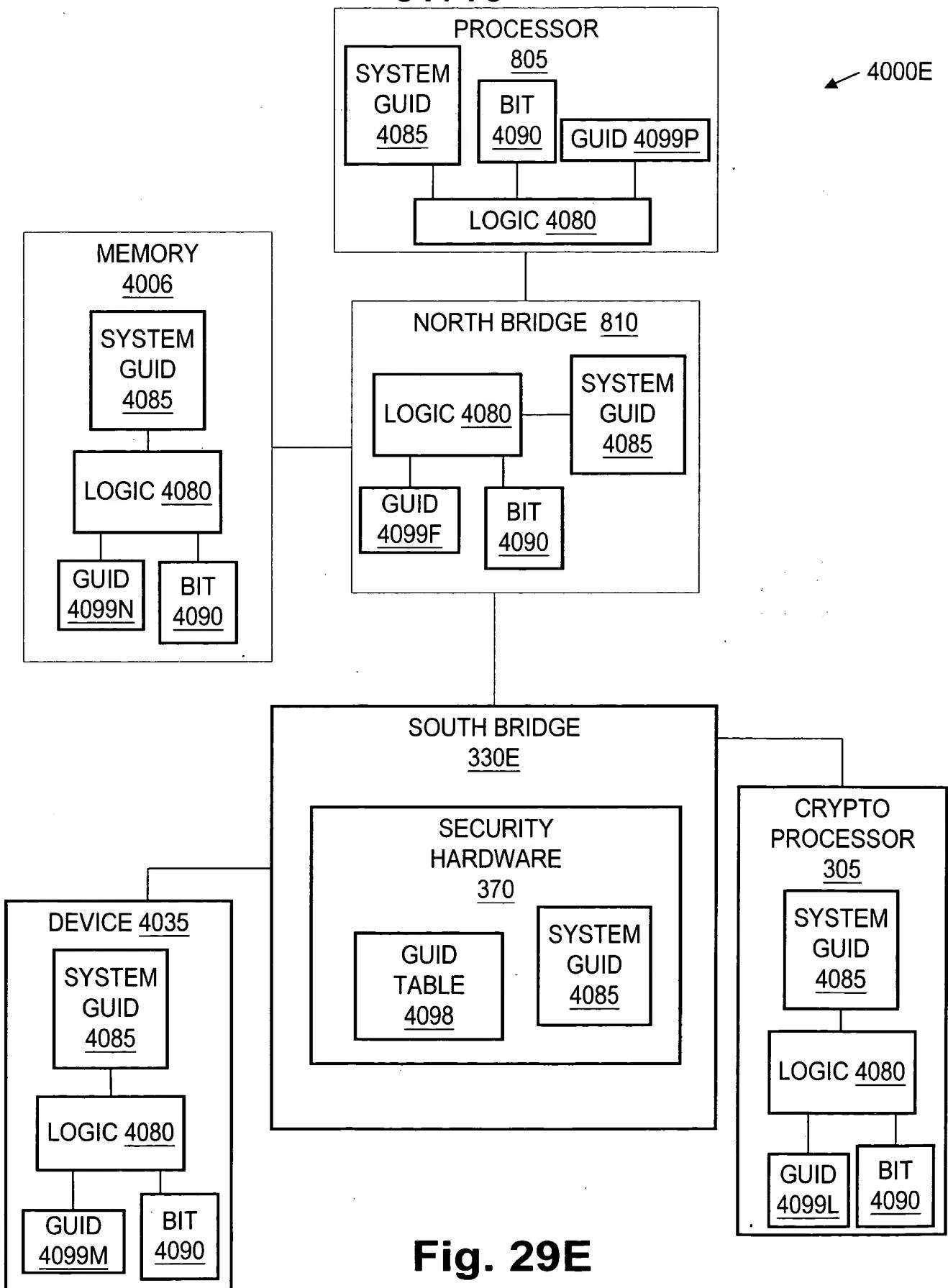


Fig. 29E

4100A

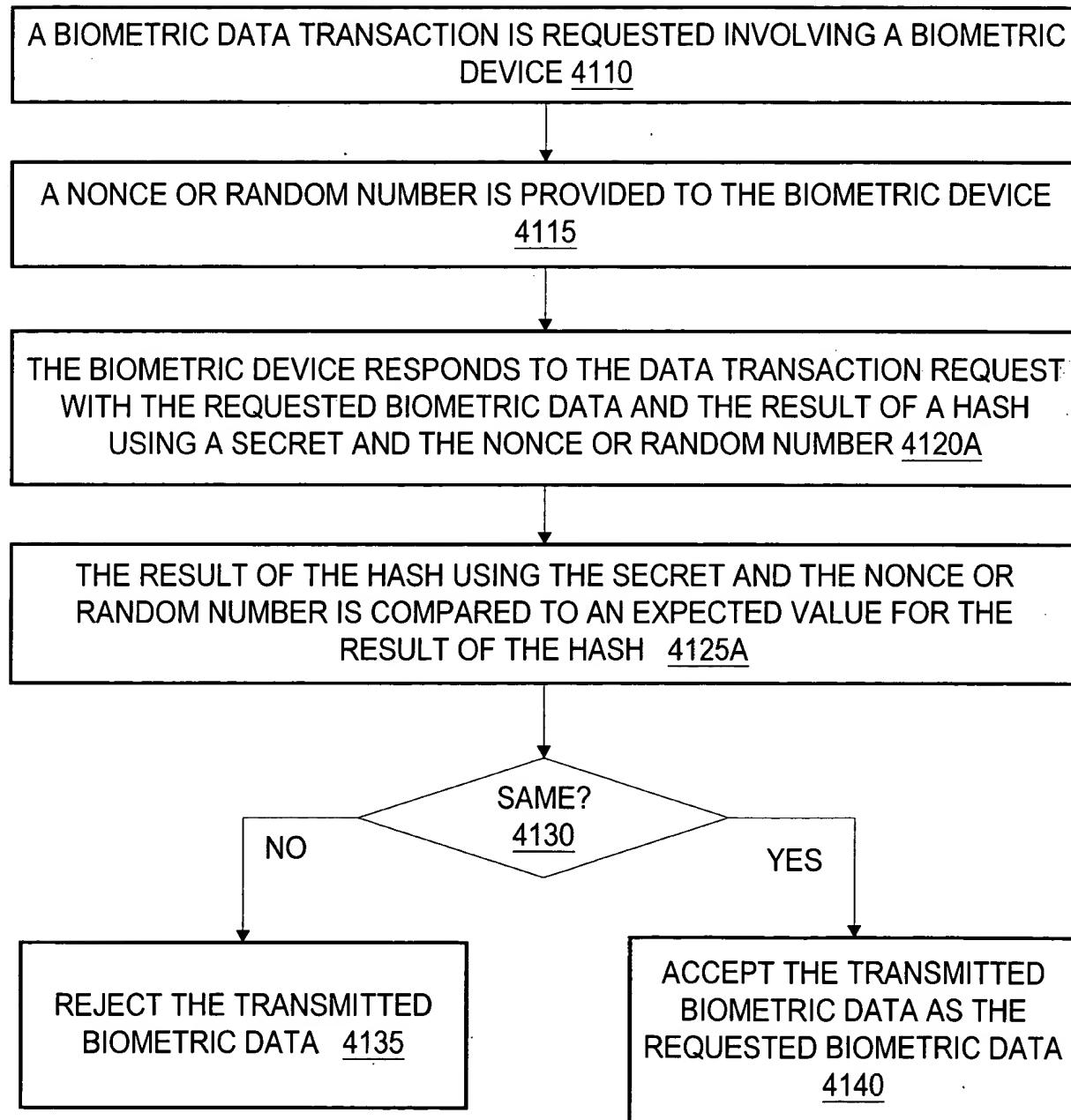


Fig. 30A

4100B

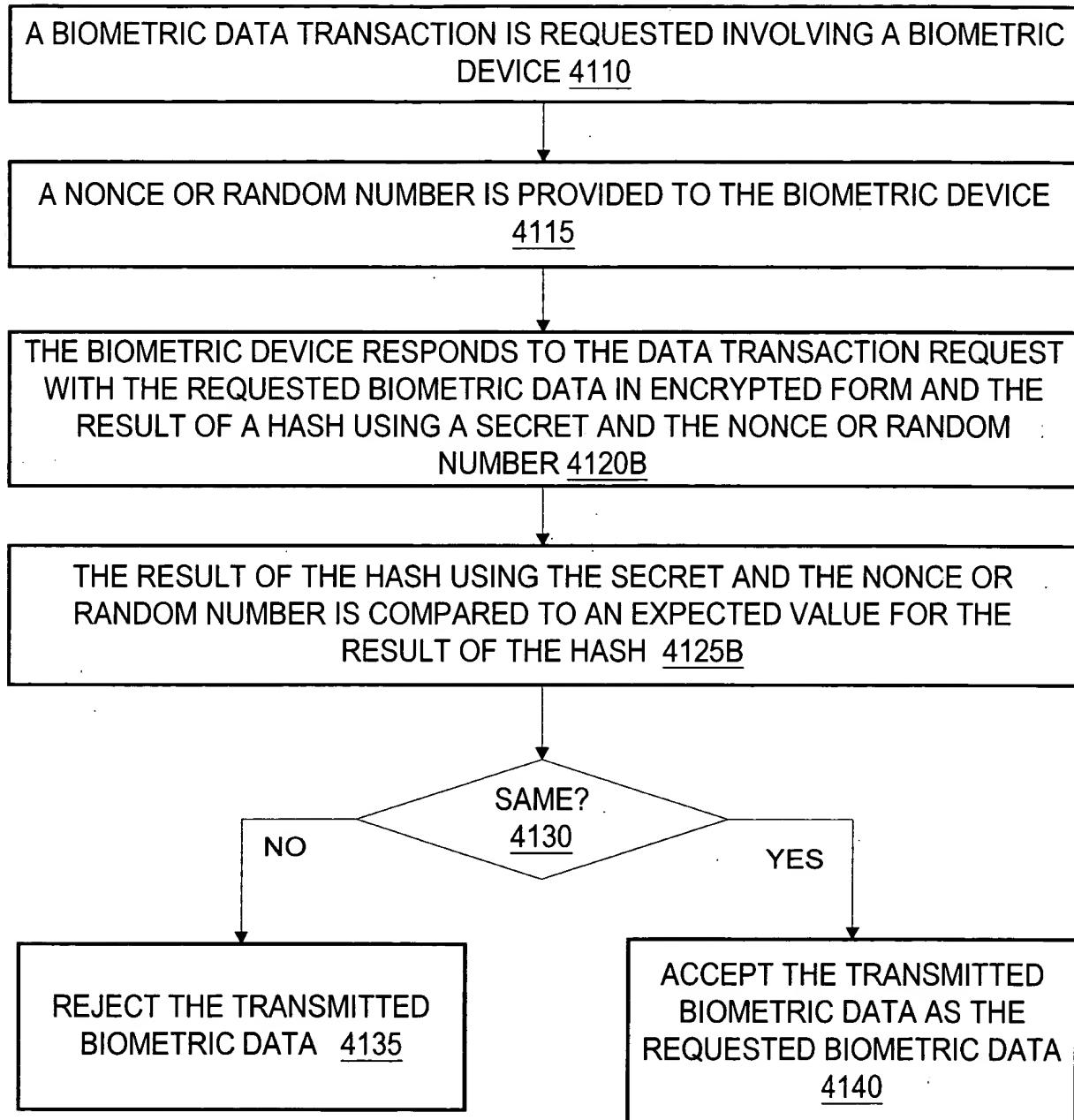


Fig. 30B

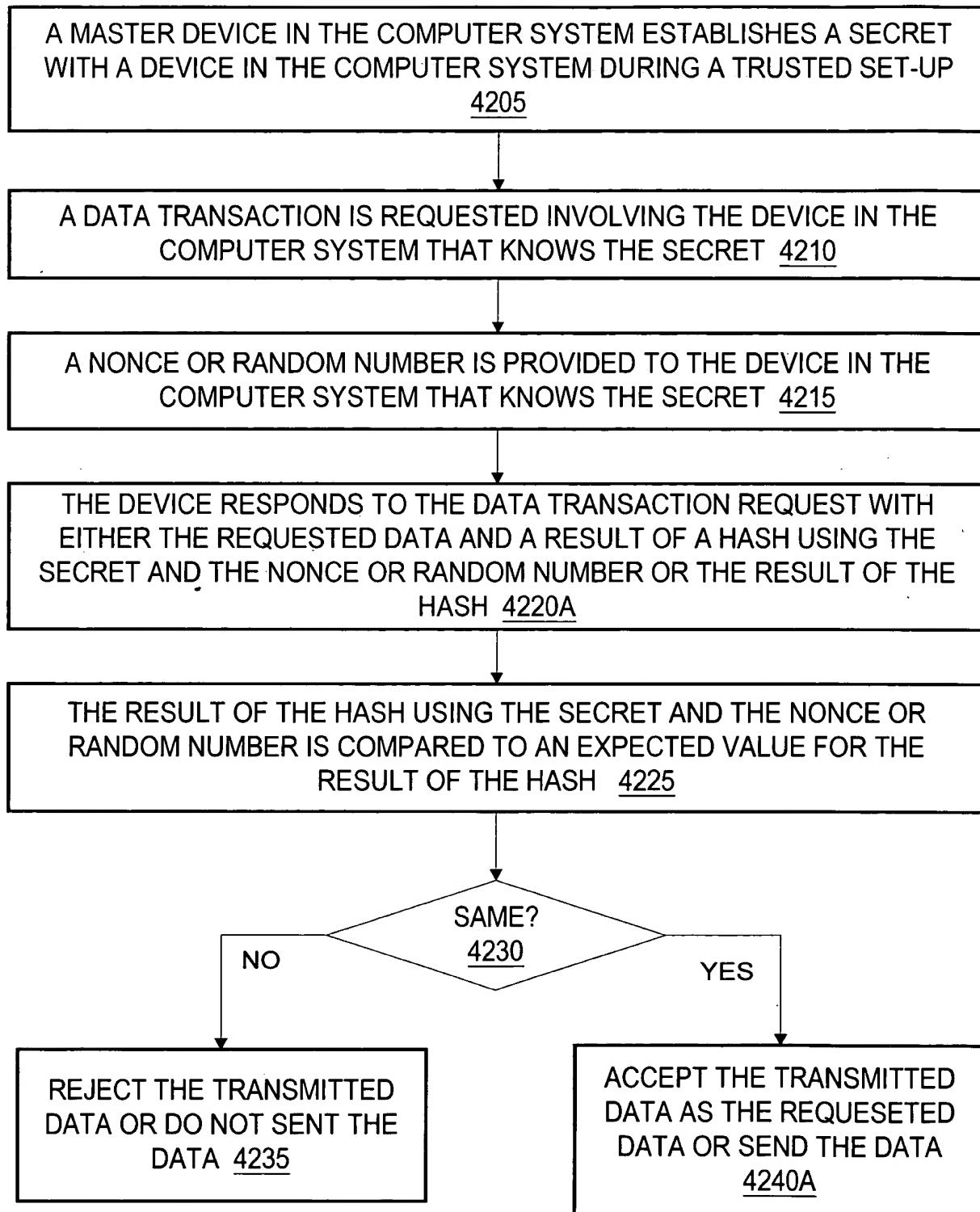


Fig. 31A

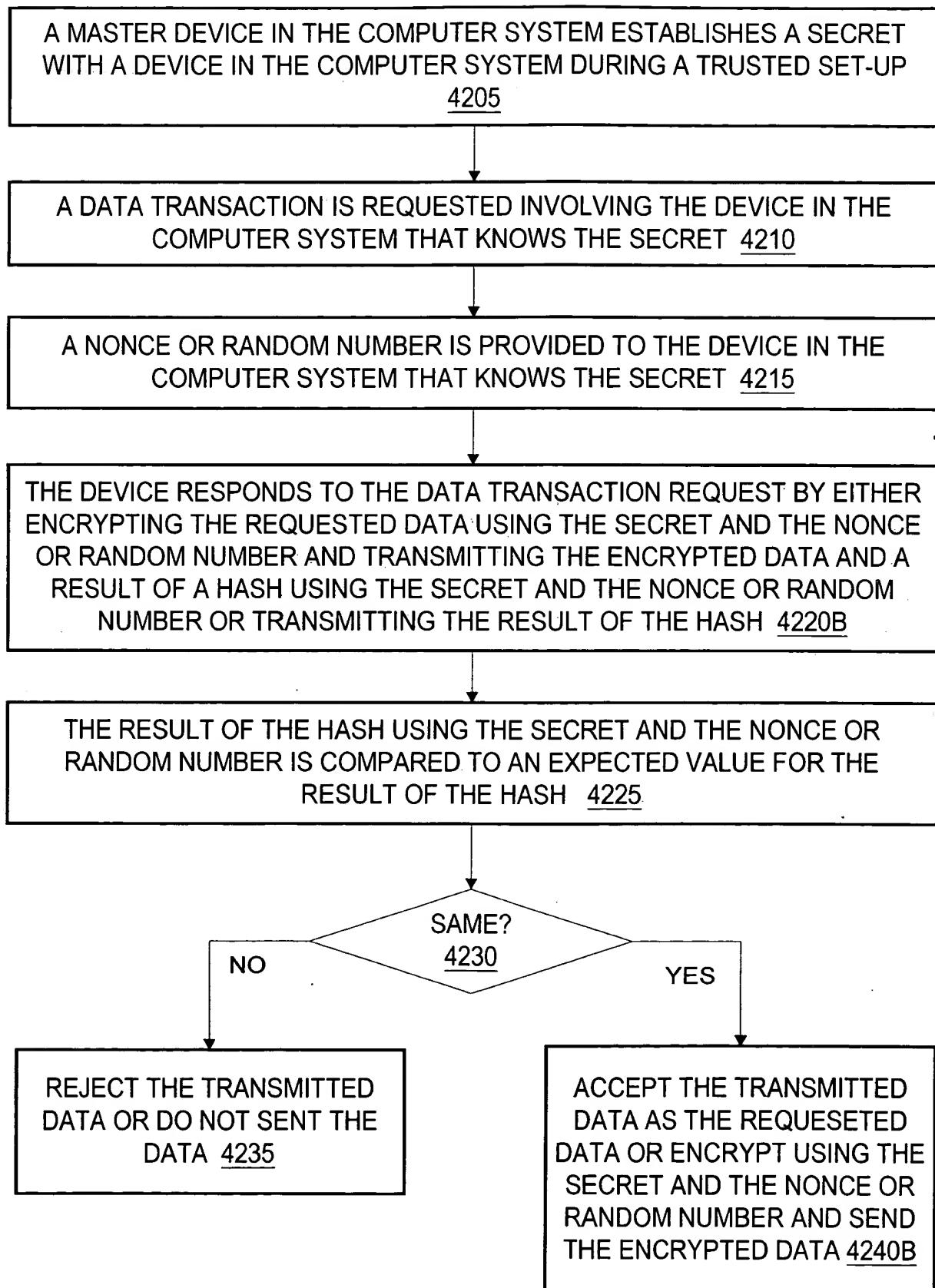


Fig. 31B

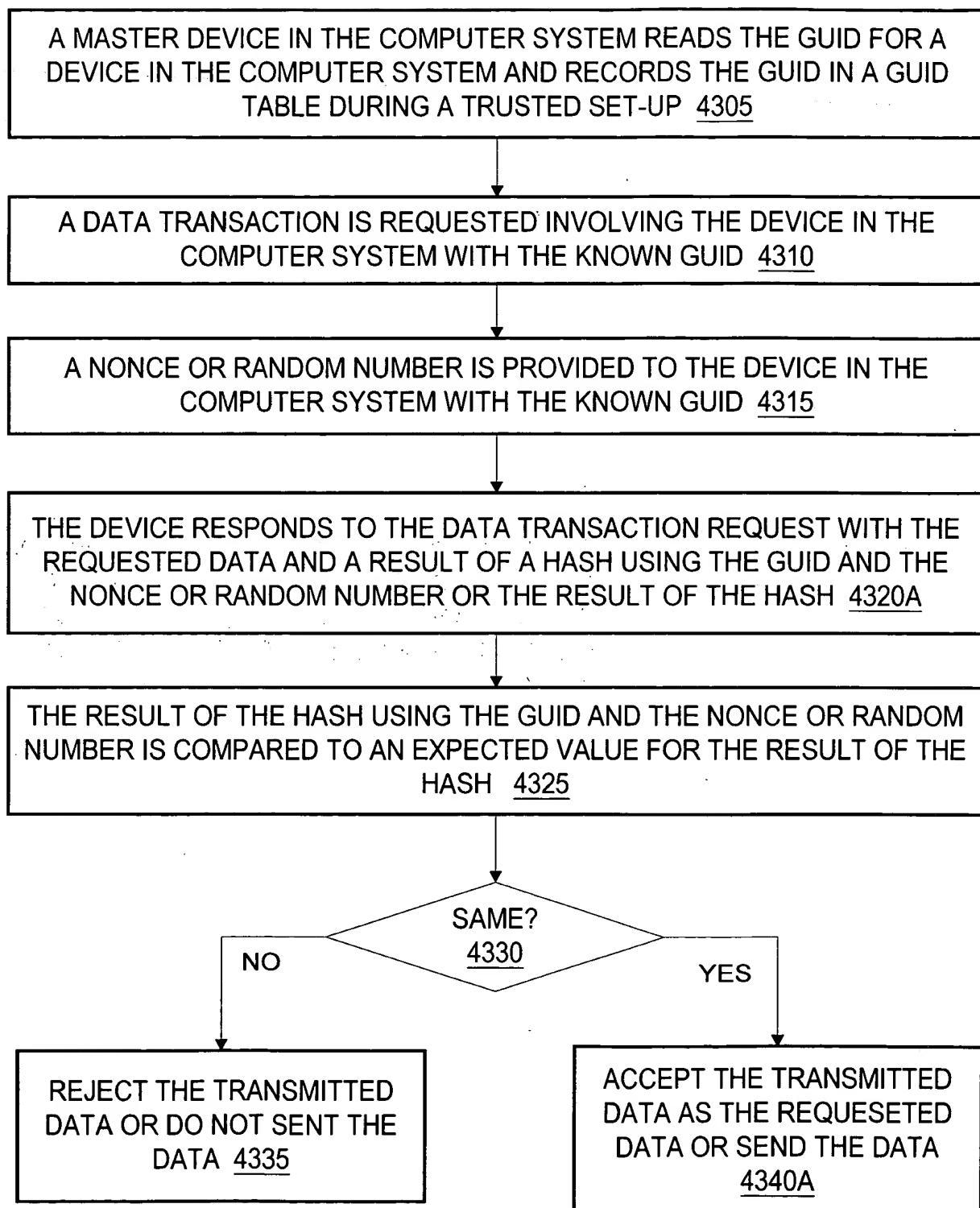


Fig. 32A

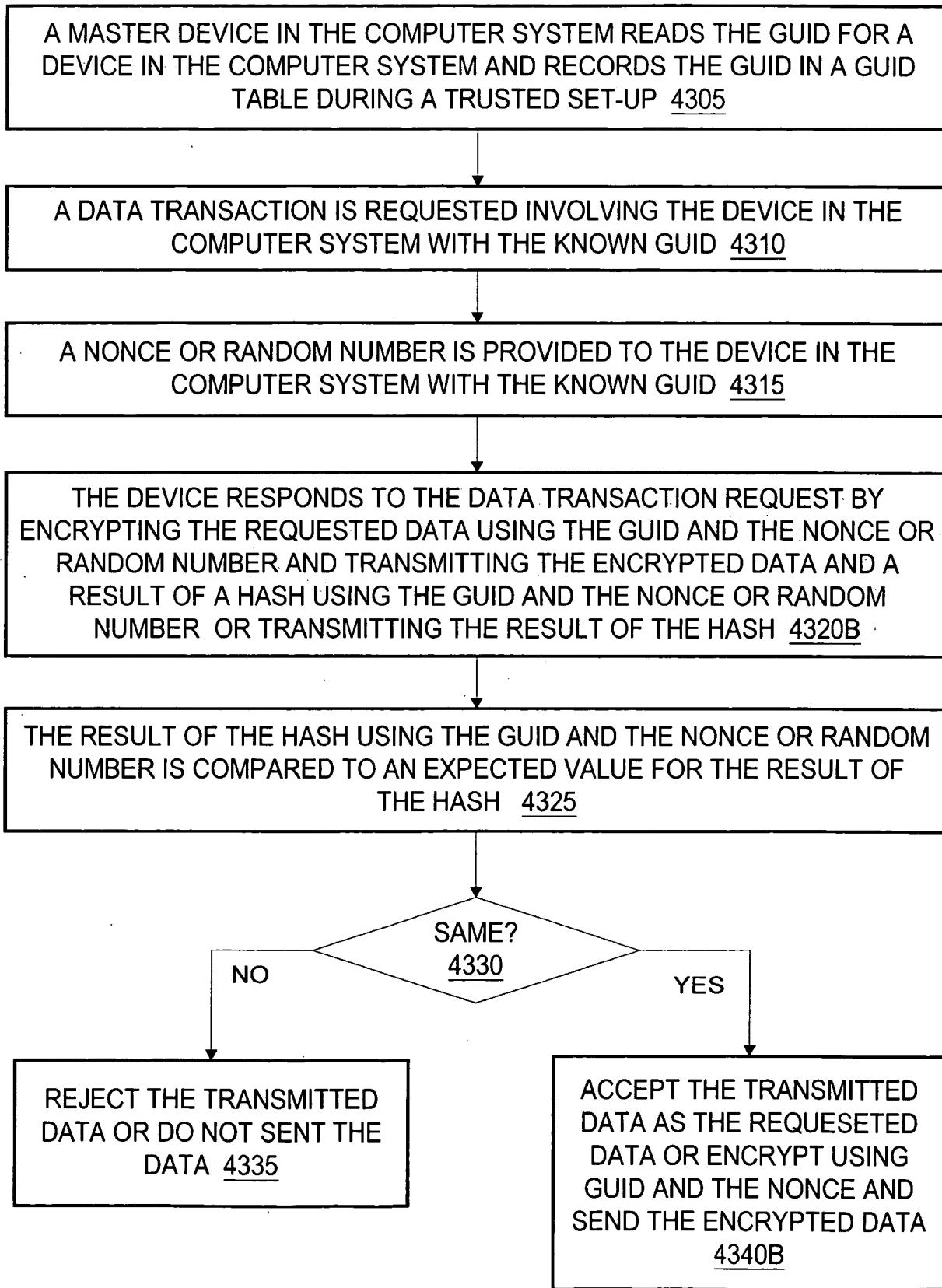


Fig. 32B

A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM, RECORDS THE GUID IN A GUID TABLE, AND TRANSMITS A SECRET TO THE DEVICE DURING A TRUSTED SET-UP

4306

A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET

4311

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET

4316

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320C

THE RESULT OF THE HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4326

SAME?

4330

NO

YES

REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335

ACCEPT THE TRANSMITTED DATA AS THE REQUESTED DATA OR ENCRYPT USING THE SECRET, THE GUID, AND THE NONCE AND SEND THE ENCRYPTED DATA 4340C

Fig. 32C

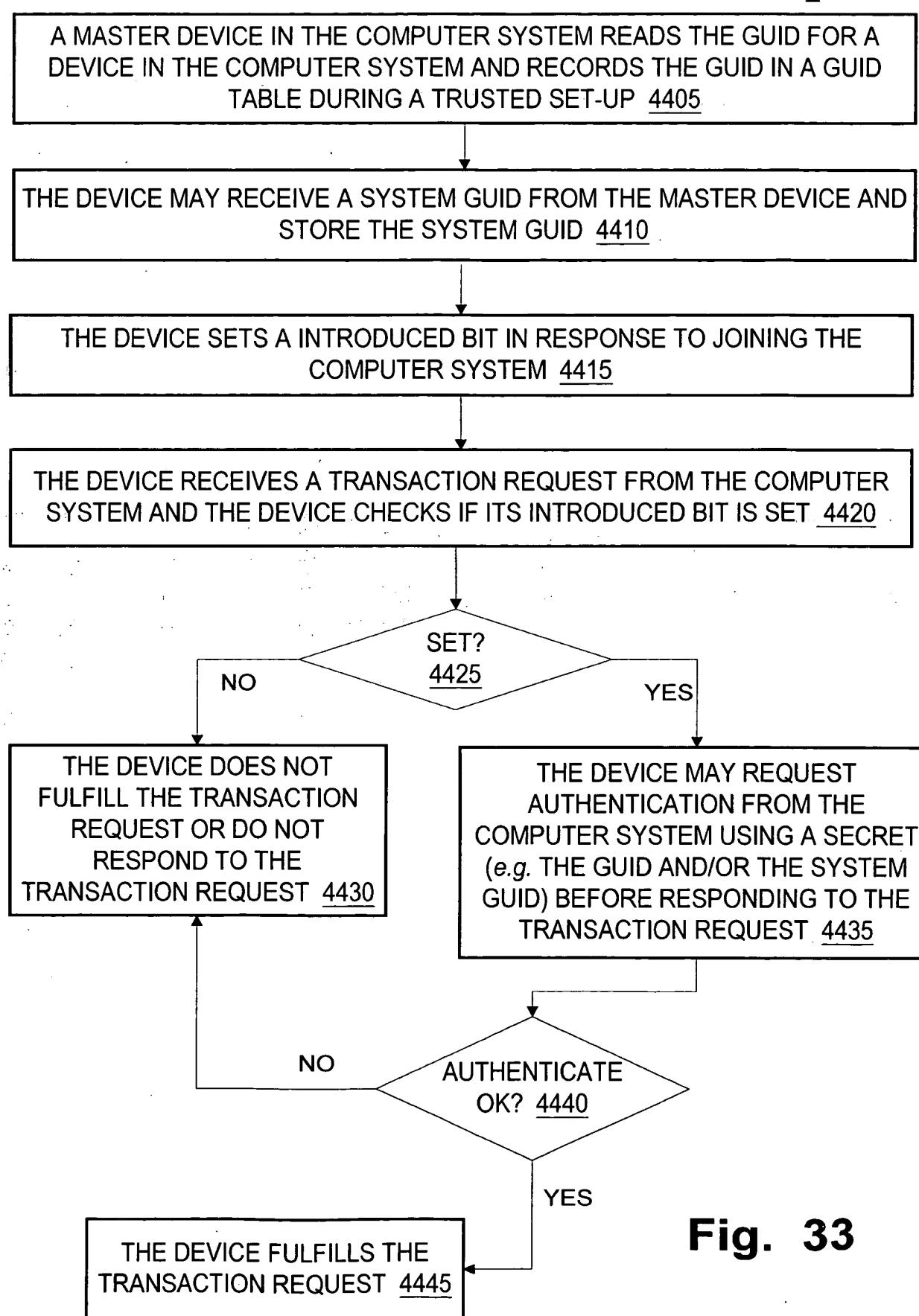


Fig. 33

63 / 73

4500

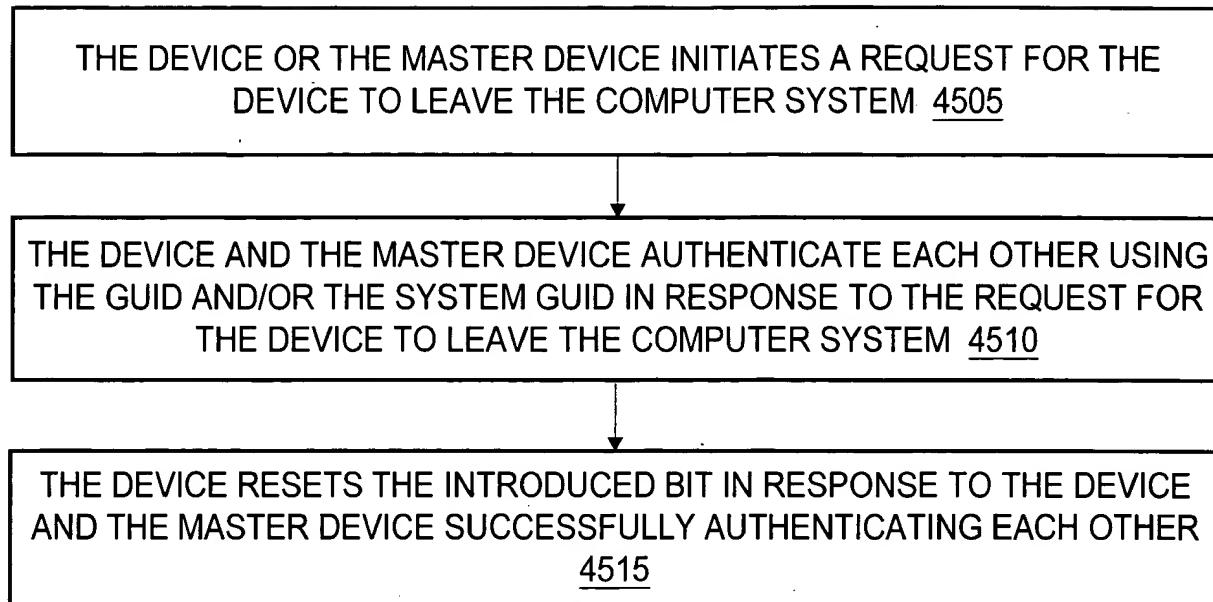


Fig. 34

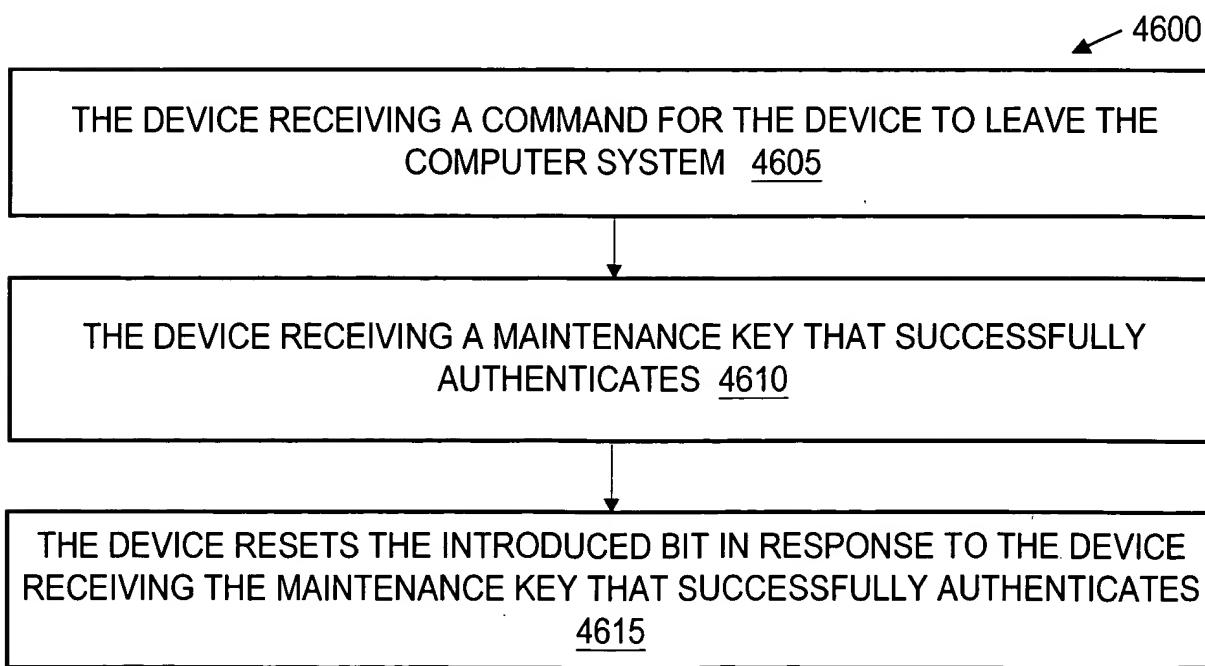


Fig. 35

64 / 73

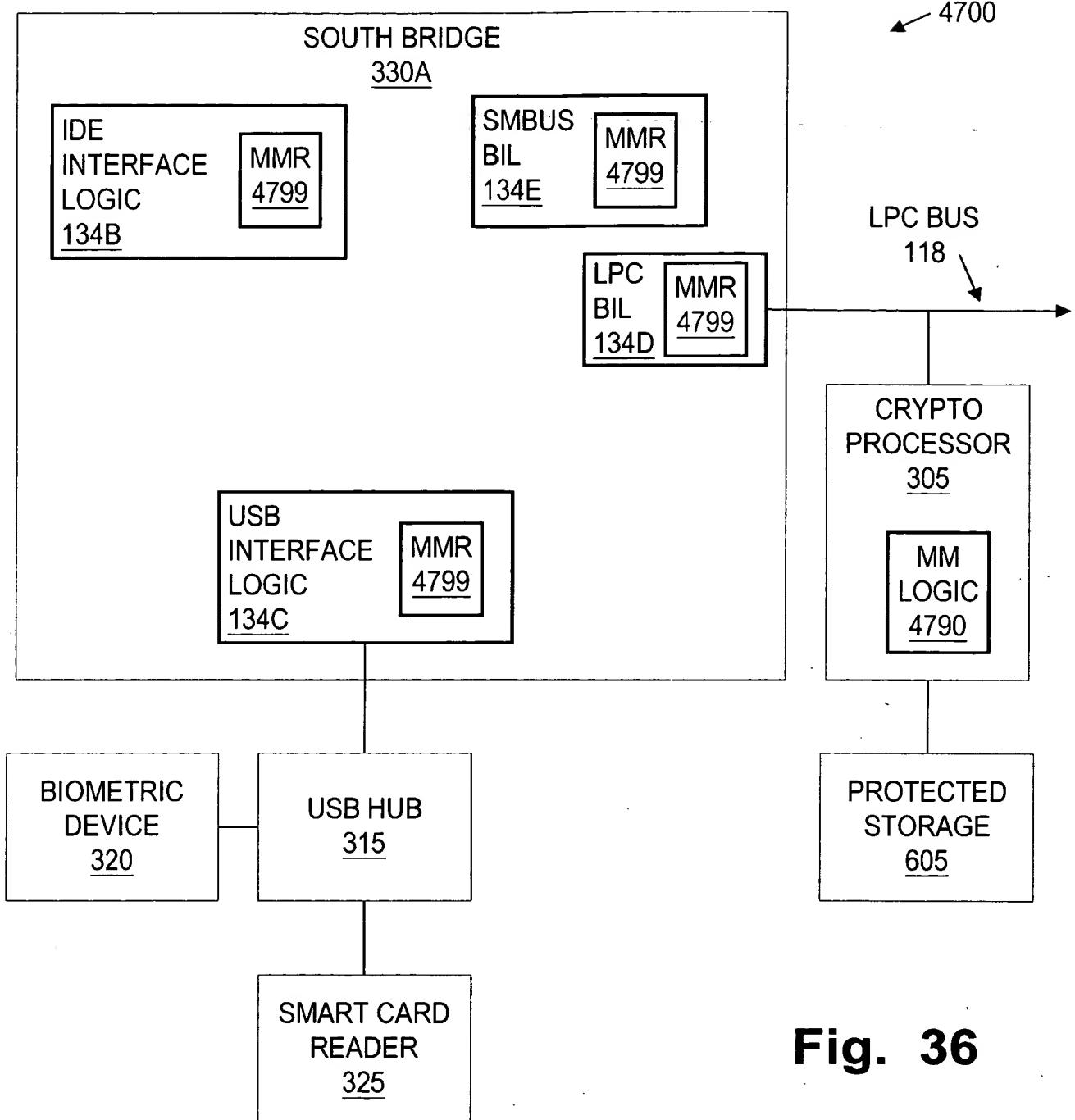


Fig. 36

TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER

4805

SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM 4810

THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4815

THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS 4820

THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE Maser MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER

4825

Fig. 37

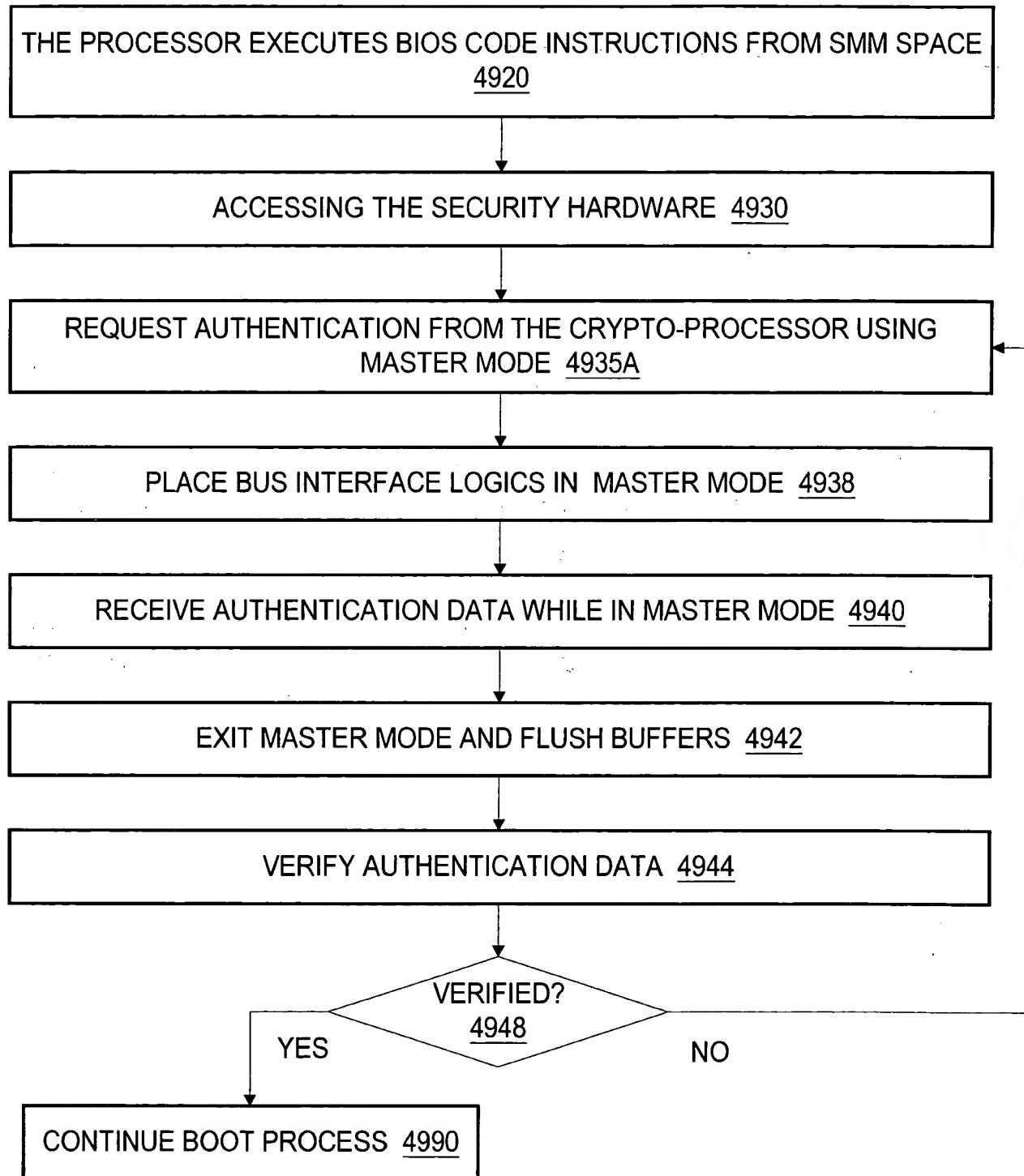


Fig. 38A

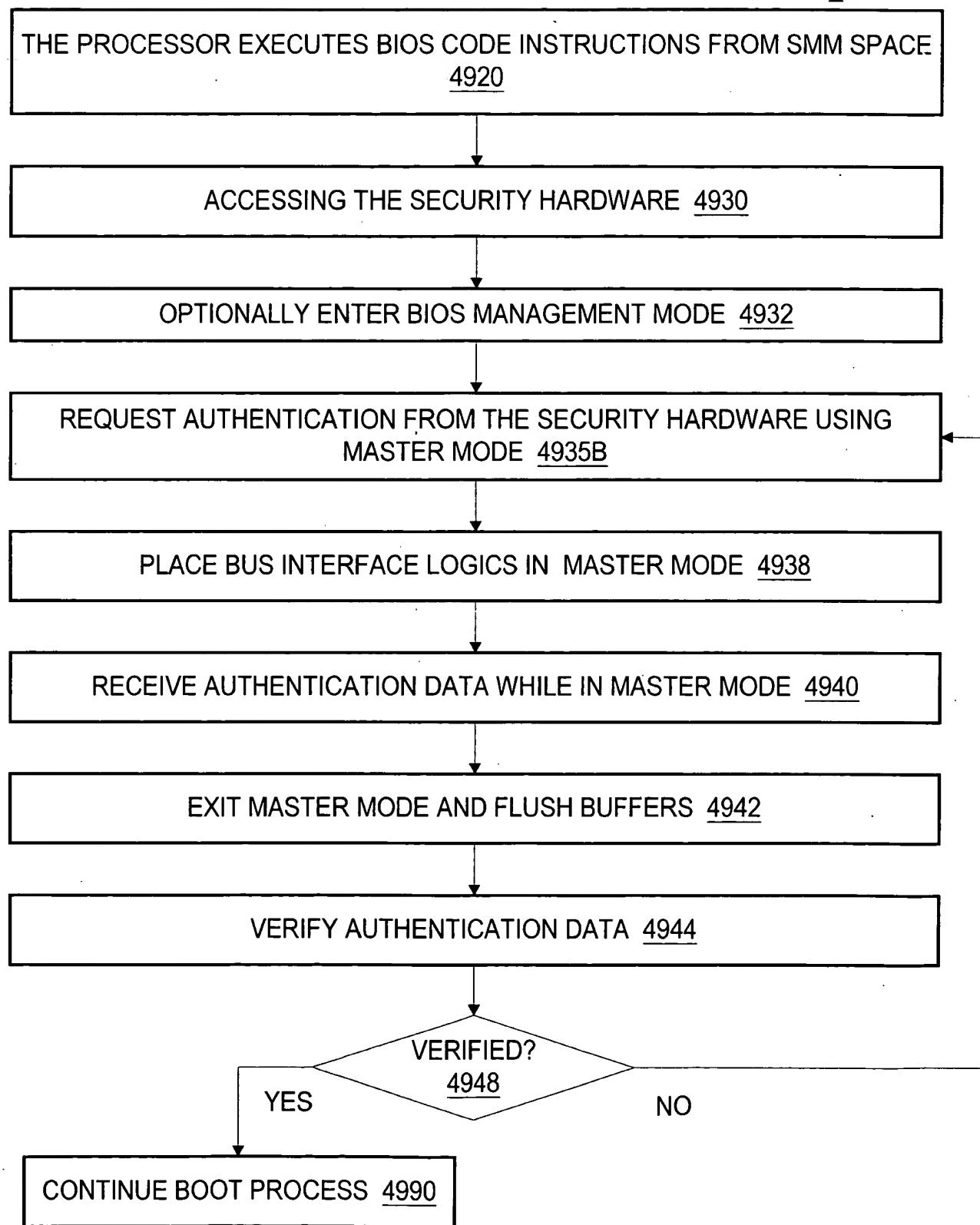


Fig. 38B

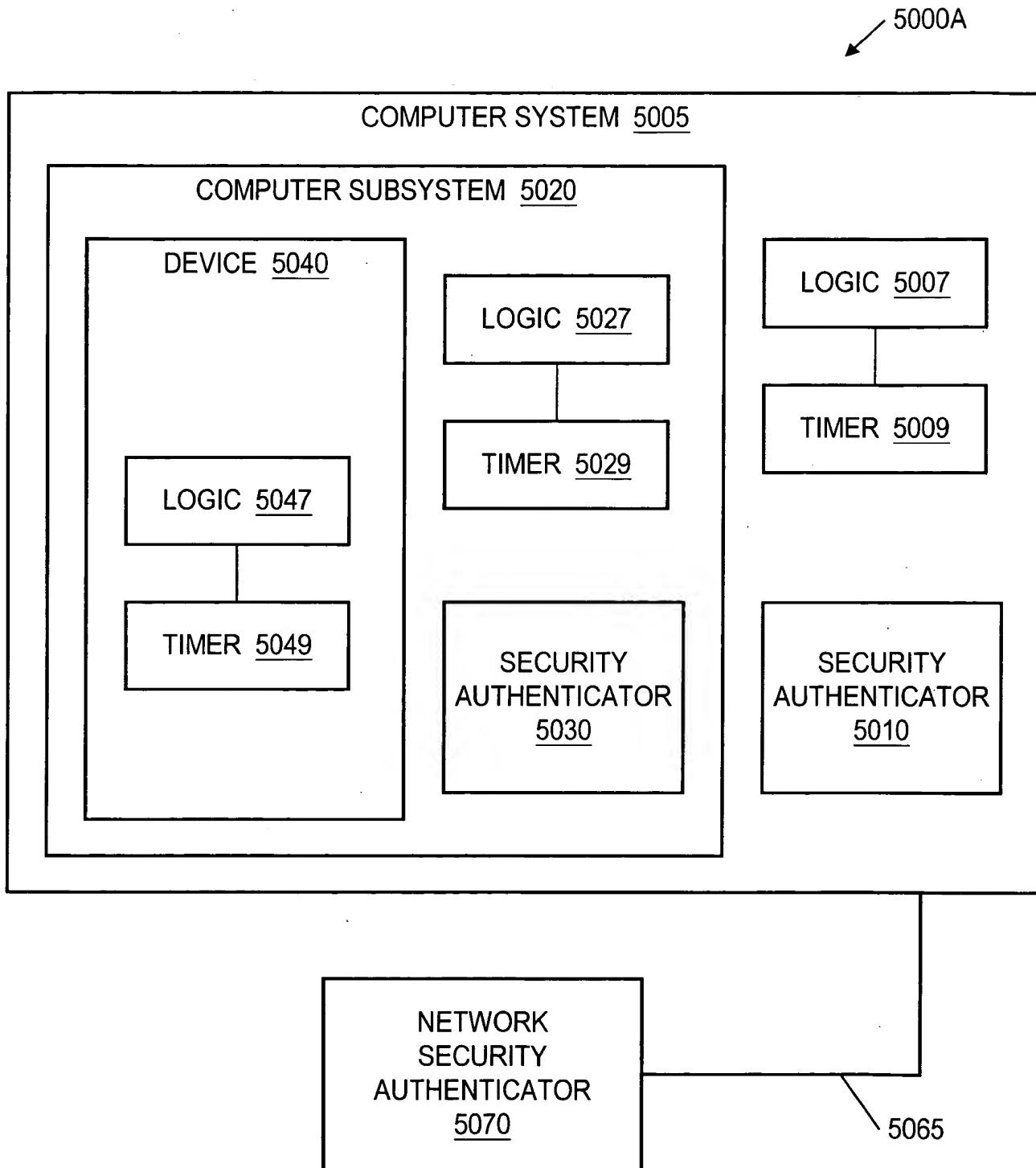


Fig. 39A

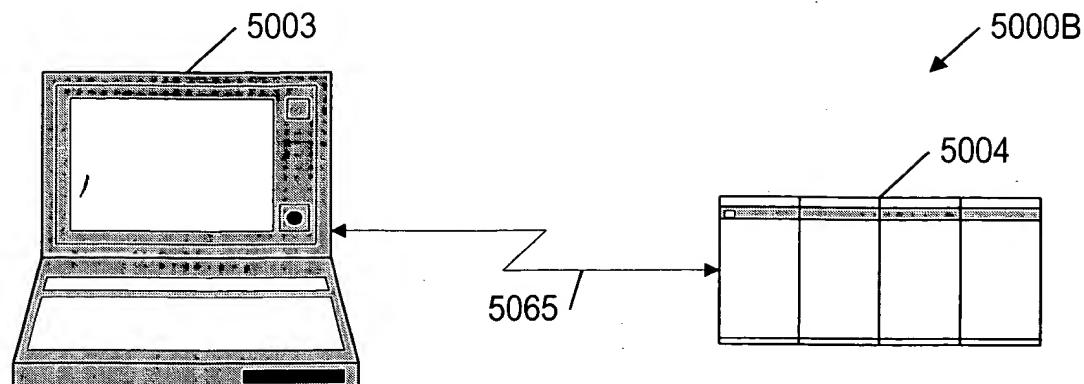


Fig. 39B

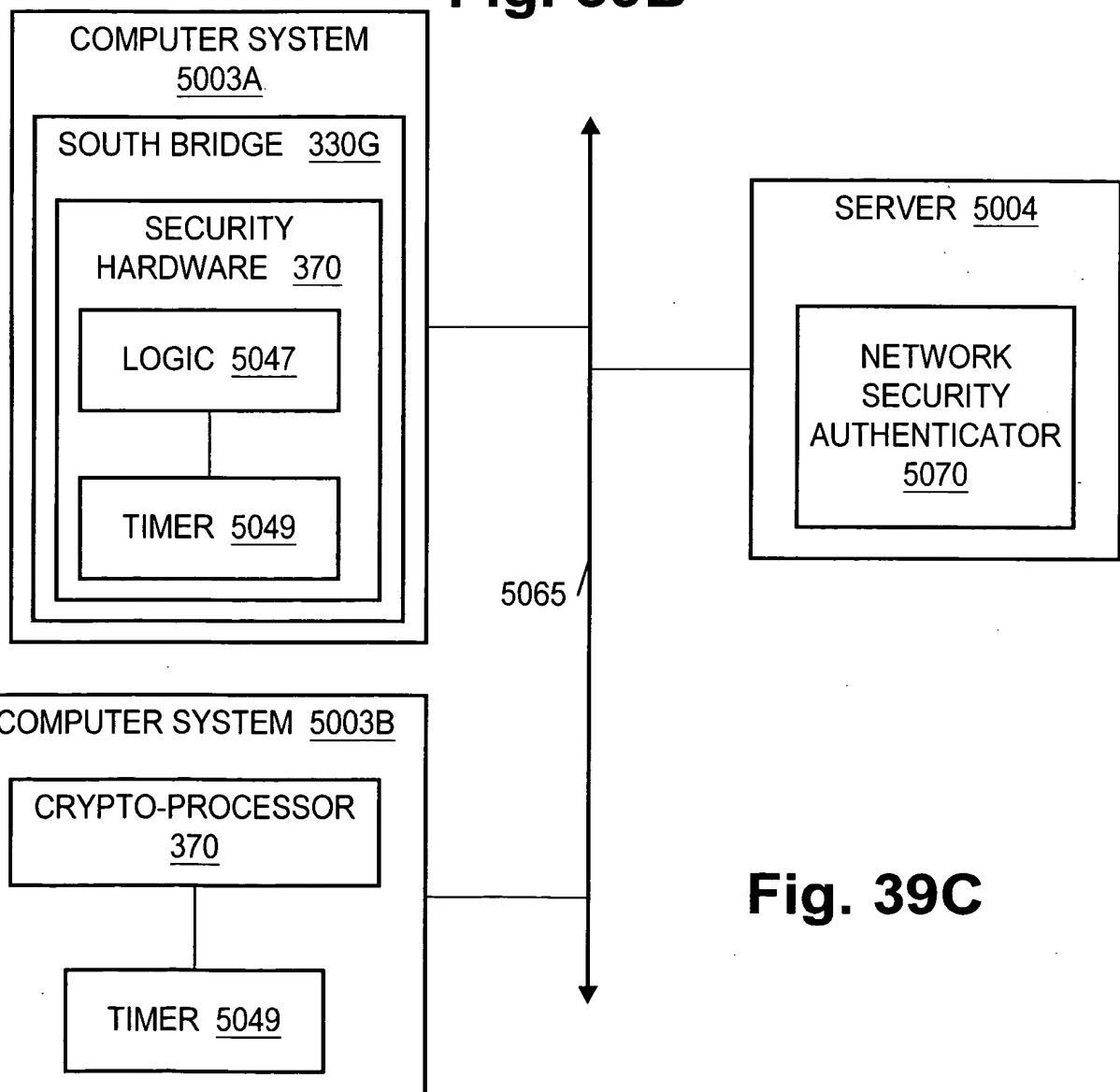


Fig. 39C

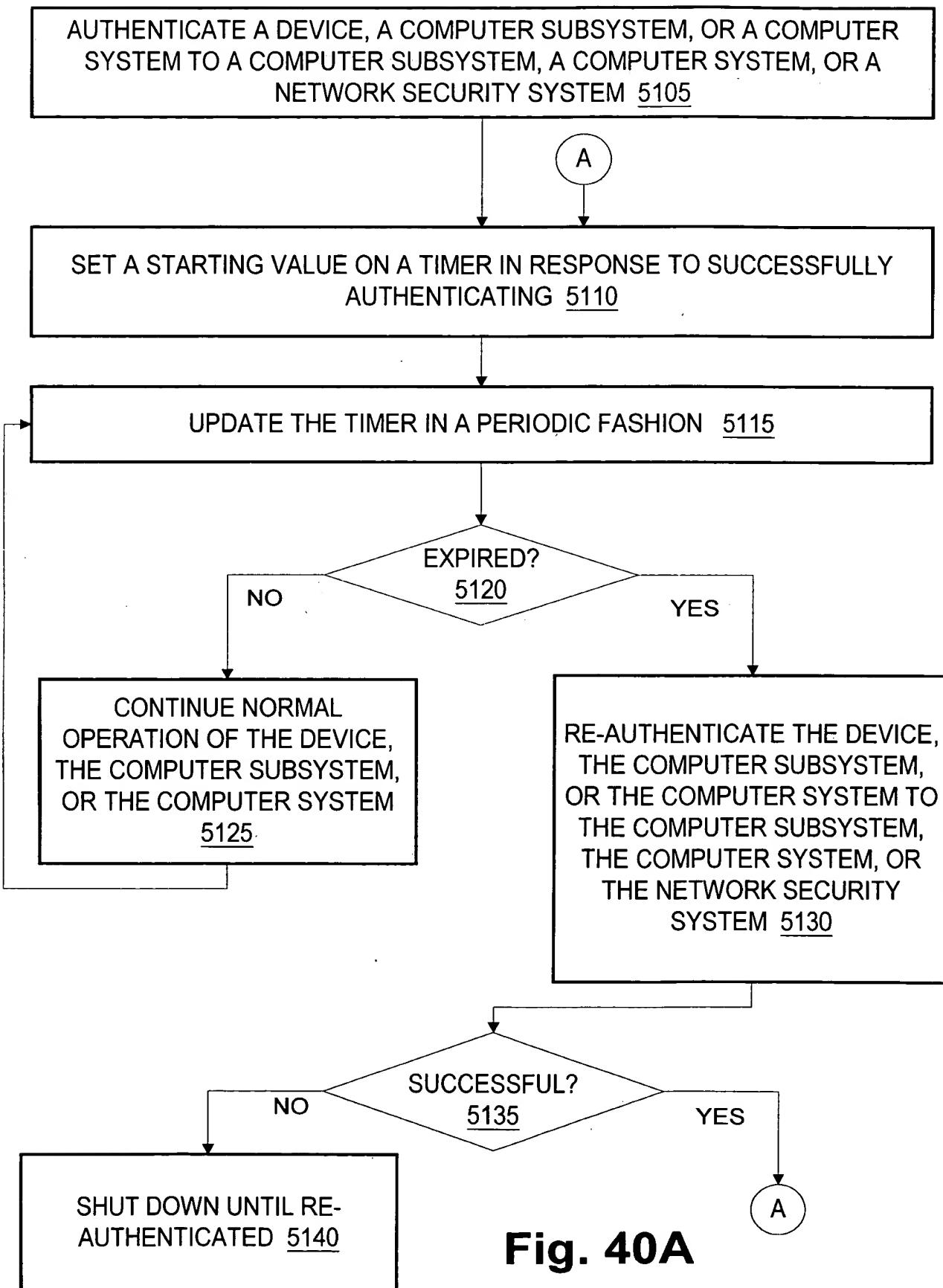


Fig. 40A

71 / 73

5100B

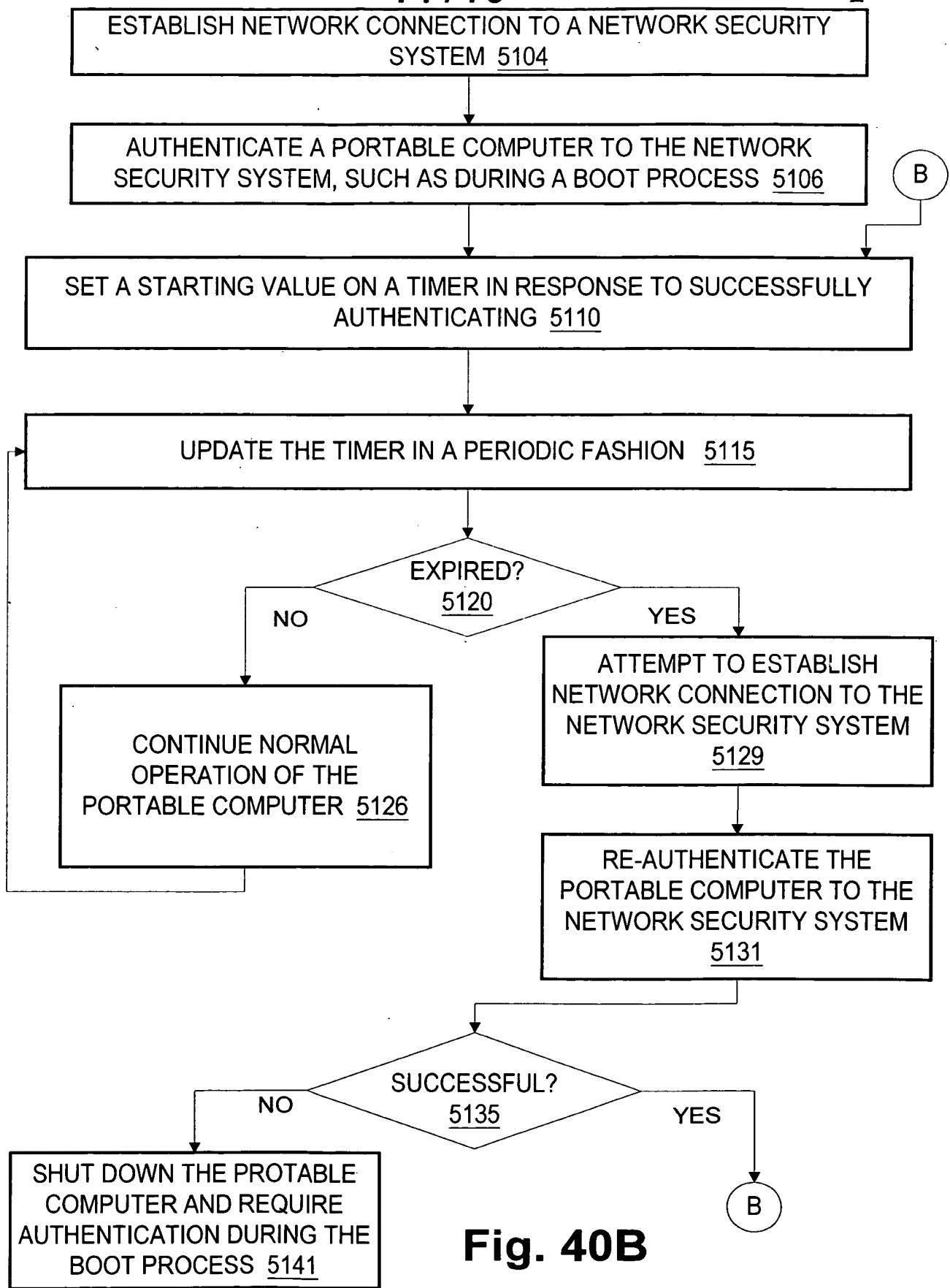


Fig. 40B

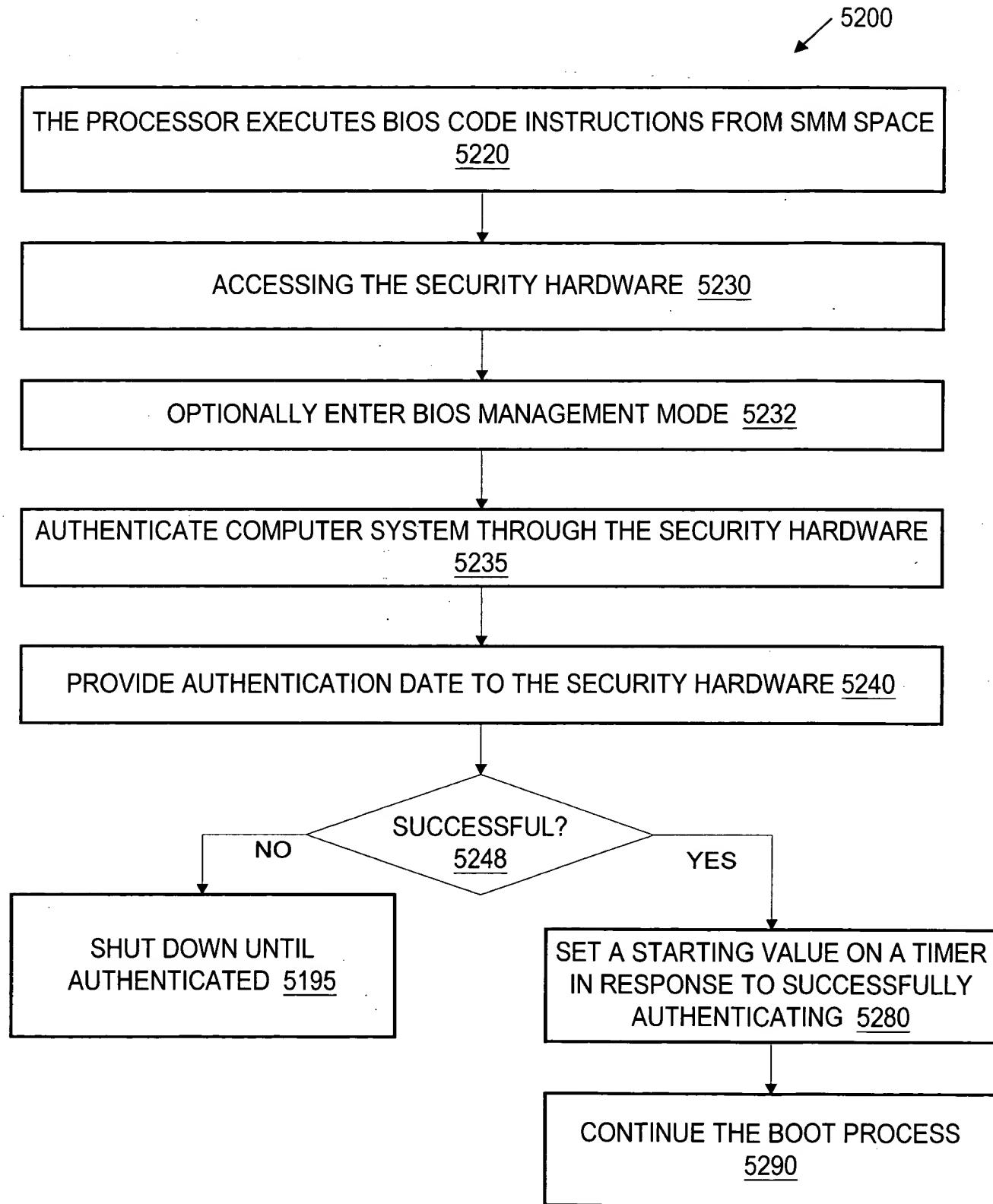


Fig. 41

73 / 73

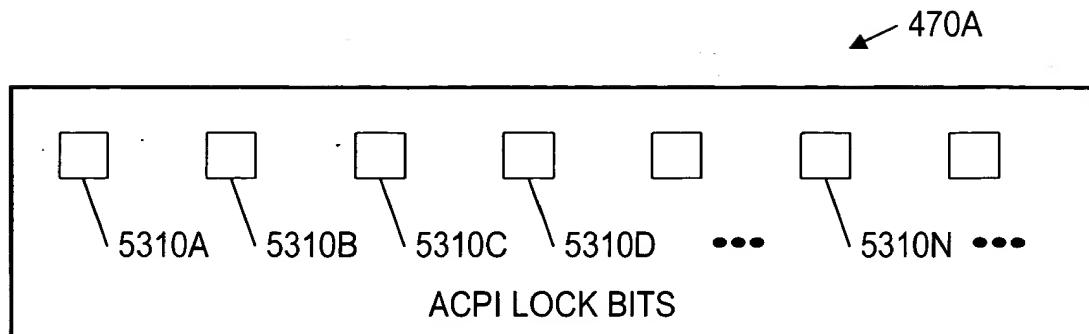


Fig. 42A

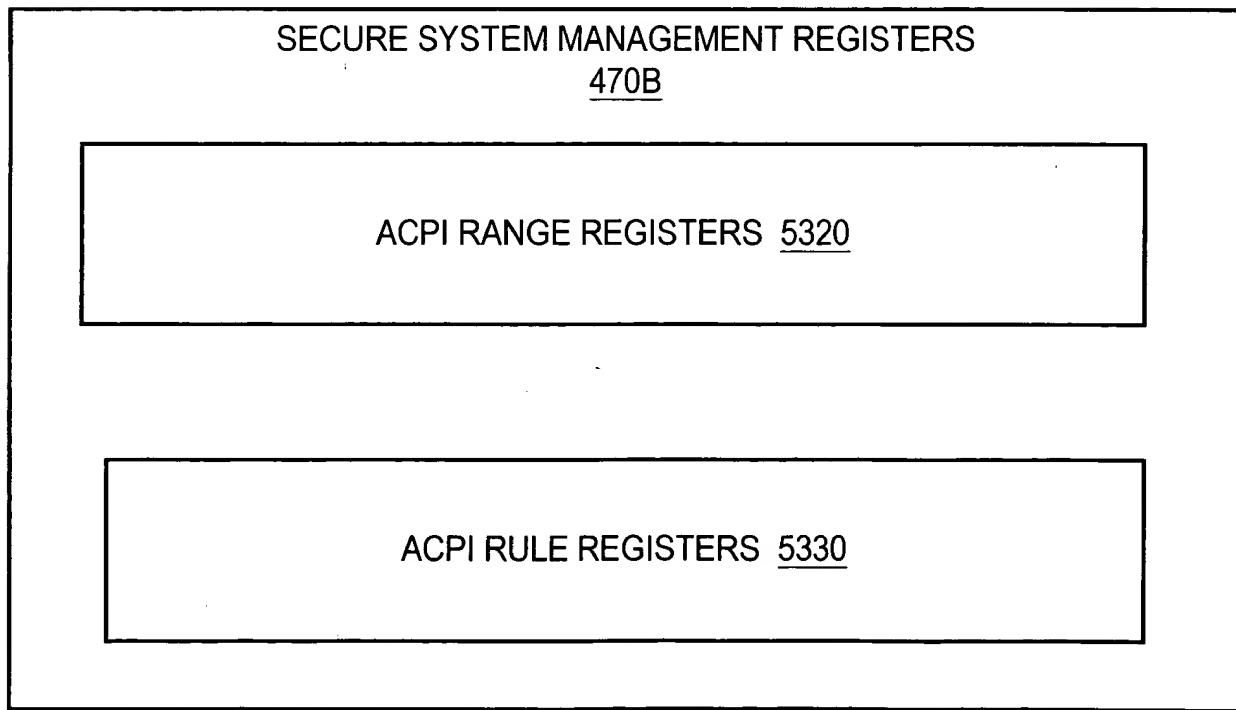


Fig. 42B